UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:
Ingeniera e Ingeniero de Sistemas

TEMA:

DESARROLLO DE UNA PROPUESTA PARA LA IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE DENTRO DEL CENTRO DE PROCESAMIENTOS DE DATOS (CPD) DE LA CARRERA DE INGENIERÍA DE CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD POLITÉCNICA SALESIANA CAMPUS SUR.

AUTORES:
DIEGO JAVIER CARRILLO VINUEZA
DIANA KAROLINA CORTEZ OVIEDO

TUTOR:
WALTER FERNANDO GAIBOR NARANJO

Quito, julio del 2019

CESIÓN DE DERECHOS DE AUTOR

Nosotros, Diego Javier Carrillo Vinueza, con documento de identificación N° 1718255456, y Diana Karolina Cortez Oviedo, con documento de identificación N° 1718684192, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación con el tema: "DESARROLLO DE UNA PROPUESTA PARA LA IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE DENTRO DEL CENTRO DE PROCESAMIENTOS DE DATOS (CPD) DE LA CARRERA DE INGENIERÍA DE CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD POLITÉCNICA SALESIANA CAMPUS SUR", mismo que ha sido desarrollado para optar por el título de INGENIEROS DE SISTEMAS en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

.....	.....
DIANA KAROLINA CORTEZ OVIEDO	DIEGO JAVIER CARRILLO VINUEZA
CI: 1718684192	**CI:** 1718255456

Quito, julio del 2019

DECLARATORIA DE COAUTORÍA DEL TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el proyecto técnico, con el tema: "DESARROLLO DE UNA PROPUESTA PARA LA IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE DENTRO DEL CENTRO DE PROCESAMIENTOS DE DATOS (CPD) DE LA CARRERA DE INGENIERÍA DE CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD POLITÉCNICA SALESIANA CAMPUS SUR", realizado por Diego Carrillo y Karolina Cortez, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, julio 2019

.....

WALTER FERNANDO GAIBOR NARANJO

CI: 1713106647

DEDICATORIA

Dedico este trabajo en primer lugar a mi madre que ha sido un soporte en todo momento con su amor, comprensión y apoyo durante toda mi vida y por ayudarme con todos los recursos para seguir con mi educación. Han sembrado en mí todos mis valores, mis principios, mi perseverancia y mi coraje para llegar a todas las metas que me proponga.

A mis hermanos Moraima y Alex por la compañía, comprensión y apoyo incondicional, por sus consejos y por su compañía que son una fuente de motivación, inspiración y felicidad en mi vida.

Diego Javier Carrillo Vinueza

Mi tesis la dedico con todo mi amor y cariño a mi madre Marianita de Jesús a mi Padre Galo a mis hermanos Carlos e Ivonne y sobre todo a mi hijo Alejandro, por darme apoyo, tiempo y fuerzas para alcanzar mis objetivos trazados ya que son la parte esencial de mi camino.

Diana Karolina Cortez Oviedo

AGRADECIMIENTO

Agradecemos a la Universidad Politécnica Salesiana que ha contribuido en nuestra formación profesional y personal, a nuestro tutor de proyecto de titulación el Ingeniero Walter Fernando Gaibor Naranjo por habernos orientado y motivado para poder realizar nuestro trabajo.

Autores Diego y Karolina

ÍNDICE

INTRODUCCIÓN **1**

Problema de Estudio 2

Justificación 3

Objetivo general 4

Propuesta de Solución y Alcance 5

Metodología 5

Capítulo 1…. 8

1.1 Informática Forense 8

2.1.1 Computación Forense (Computer Forensics) 8

1.1.2 Forensic en Redes (Network Forensics) 9

1.1.3 Forensia Digital (Digital Forensics) 9

1.2 Ciencias Forenses 9

1.3 Antecedentes de delitos informáticos 10

1.4 Script Kiddies 11

1.5 Hackers 11

1.6 Tipos de delitos informáticos 11

1.6.1 Ciberacoso (Cyberbullying) 11

1.6.2 Robo de identidad 12

1.6.3 Secuestro de datos (Ransomware) 12

1.7 Principios básicos para el manejo de pruebas digitales 12

1.8 Sustento de pruebas 13

1.9 Delitos Informáticos en Ecuador 14

1.10 La tipificación del delito informático en la Ley penal ecuatoriana 14

1.11 ISO 27037:2012 17

1.12 Criptografía 18

Capítulo 2…. 19

2.1 Antecedentes de la infraestructura inicial 19

2.2. Inventarios de Laboratorios de la Carrera de Computación 19

2.2.1 Laboratorio de Networking 1 19

2.2.2 Laboratorio de Networking 2 21

2.2.3 Laboratorio de Networking 3 29

2.2.4 Laboratorio de Computación Avanzada 30

2.2.5 Laboratorio IHM (Interacción Humano Máquina) 31

2.3 Laboratorio de Informática Forense UPS 37

Capítulo 3…. 39

3.1 Consideraciones generales para la implementación 39

3.2 Prácticas de investigación y análisis forense para el laboratorio de la Carrera de Computación 39

3.2.1 Identificación de la ubicación de un ataque Phishing a través de un correo electrónico 39

3.2.2 Análisis de imágenes digitales mediante herramienta WEB FOTOFORENSICS 43

3.2.3 Denegación de Servicios utilizando la herramienta HOIC 47

3.2.4 Análisis y recuperación de archivos eliminados de un dispositivo de almacenamiento..... 52

3.2.5 Creación de imagen a partir de una unidad de almacenamiento..... 58

3.2.6 Estudio Forense de Archivos Multimedia en WHATSAPP 61

3.2.7 Estudio de imagen de una unidad de acopio externo con la herramienta Autopsy 66

3.2.8 Análisis de Información de una PC con sistema operativo Windows mediante herramienta OSForencis..... 70

3.2.9 Estudio de Memoria RAM con Volatility Framework en KALI-LINUX 75

3.2.10 Análisis de eventos de sistemas operativo mediante la Herramienta Event Log Explorer..... 79

3.3 Herramientas de software para implementar en el Laboratorio de Informática Forense 83

3.4 Propuesta para la Adquisición de Hardware y software especializado para el Laboratorio de Informática Forense..... 85

CONCLUSIONES..... 87

RECOMENDACIONES..... 88

LISTA DE REFERENCIAS 89

ÍNDICE DE TABLAS

Tabla 1. Laboratorio Networking 1 20
Tabla 2. Inventario de Software Laboratorio de Networking 1 21
Tabla 3. Inventario Laboratorio de Networking 2 22
Tabla 4. Inventario de Software Laboratorio de Networking 2 23
Tabla 5. Equipos de Networking 24
Tabla 6. Inventario Laboratorio de Networking 3 29
Tabla 7. Inventario Laboratorio de Computación Avanzada 30
Tabla 8. Inventario Laboratorio IHM 31
Tabla 9. Inventario Software IHM 32
Tabla 10. Inventario Tabletas Android 32
Tabla 11. Inventario Tabletas Apple 33
Tabla 12. Registro de servidores APOLLO 6000 HPE 34
Tabla 13. Registro de STORAGE 3PAR 8200 35
Tabla 14. Registro de SWITCH SAN 35
Tabla 15. Radio de 2 vías 36
Tabla 16. Monitor 49INC LH49PMHP Series EDGE-LIT LED 36
Tabla 17. Televisor LED 4K 36
Tabla 18. Impresora L575 37
Tabla 19. Eventos más importantes. 80
Tabla 20. Software utilizado 84
Tabla 21. Software para análisis forense 85
Tabla 22. Hardware para análisis forense. 86

ÍNDICE DE FIGURAS

Figura 1. Esquema Investigación Proyectiva 7

RESUMEN

El presente proyecto de tesis tiene como propuesta la implementación de un Laboratorio de Informática forense que permita realizar un estudio, análisis e investigación de delitos informáticos que acontecen dentro de nuestra sociedad y de esta manera aportar con evidencia digital ante procesos judiciales tipificados en el Código Orgánico Integral Penal del Ecuador, para lo cual se ha propuesto un conjunto de prácticas académicas donde se indican las herramientas y actividades a realizar en función de una situación en particular. Cabe destacar que los delitos informáticos son de toda índole sin embargo en este trabajo se ha considerado ciertos elementos que se puedan desarrollar dentro de los laboratorios de la Carrera de Ciencias de Computación, en función de la disponibilidad de hardware y software que estos manejan. Sin embargo, al final se propone un conjunto de herramientas a adquirir con el fin de consolidar y robustecer el mencionado laboratorio.

El CPD (Centro de Procesamiento de Datos) cuenta con equipos necesarios para realizar investigaciones forense utilizando diferentes técnicas de análisis de información lo que ayuda al investigador a obtener una perspectiva amplia sobre los delitos que ocurren a diario, entre estos se encuentran ataques de ingeniería social, denegación de servicio, modificación de contenidos digitales entre otros, lo que perjudica de manera directa o indirecta a la víctima, todos estos tipos de agresiones antes mencionados se analiza en las prácticas de laboratorio bajo licencias de software en versión prueba y otras libres, lo que permite identificar los posibles causales de los ataques, manteniendo la integridad de la información sin agredir a la evidencia pura que sirve como prueba probatoria ante un proceso judicial.

ABSTRACT

The proposal of this thesis project is the implementation of a forensic computer laboratory which enables the study, analysis and investigation of different cybercrimes occurred in our society, thus providing digital evidence on judicial processes established in the “Código Integral Penal” of Ecuador. For this, a set of academic practices has been proposed, where the tools and activities to be carried out are indicated according to a situation. It is worth mentioning that computer crimes are of all kinds, however, for this work, some elements able to be developed within the laboratories of the Computer Science career have been considered, based on its software and hardware availability. Nevertheless, at the end of this work, a set of tools to be acquired is proposed in order to consolidate and strengthen the aforementioned laboratory.

The CDP (Data Processing Center) has the necessary equipment to perform forensic investigations using different information analysis techniques. This helps the researcher to have a broad perspective on daily crimes. Among these crimes we can find social engineering attacks, denial of service, modification of digital content, etc. which directly or indirectly affect the victim. All these types of crimes mentioned before are analyzed in the practices in the lab and they are happening under the licensed software, some on testing version and some in free versions, this way we are able to identify the possible causes of the attacks, maintaining the integrity of the information without hurting the pure evidence that works as proof at a legal process.

INTRODUCCIÓN

En una investigación forense, es preciso recopilar suficientes evidencias, por esta razón se requiere de una buena cantidad de herramientas apropiadas para realizar dicha tarea. La intención principal es reunir en un mismo lugar, todos los instrumentos precisos para examinar la evidencia y de esta forma tener un enfoque de la agresión informática que se esté considerando.

En el capítulo 2, se analiza conceptos relacionados a la computación forense, antecedentes, ejemplos de infracciones informáticas, seguridad, integridad, disponibilidad, artículos del código orgánico penal ecuatoriano, entre otros temas que son de valor para el estudio de la averiguación del origen y la estructura general del contenido digital para el estudio relacionado a las agresiones que se facturan día a día.

En el capítulo 3, se topa sobre la construcción física y lógica que tiene el Centro de Procesamiento de Datos de la Universidad Politécnica Salesiana de la Carrera de Ingeniería de Ciencias de la Computación, la cual accede a identificar los instrumentos de software y hardware que logran esgrimir para la implementación del Laboratorio de Informática Forense (LIF) y de este modo se optimiza los recursos dentro de la entidad.

En el capítulo 4, se realiza prácticas relacionadas a delitos informáticos de investigación forense como: phishing, metadatos en imágenes, denegación de servicios, recuperación de archivos, creación de imágenes, extracción de información de WhatsApp, datos de PC, memoria RAM, logs, los mismos que permiten adquirir, preservar y presentar datos almacenados electrónicamente que permita resolver casos policiales o judiciales dentro de un proceso de investigación.

Problema de Estudio

El incremento de los procesos de la información implica el uso de datos (creación, manipulación y almacenamiento) y la información consigue ser perceptiva para las sociedades u estructuras de toda índole, la cual se forja mediante medios estructurados (transaccionales en BD) o no estructurados (redes sociales) entre otras y pueden ser capaces de poseer ocurrencias de seguridad. Actualmente se registran diferentes tipos de ofensivas descritos como delitos informáticos o delincuencia informática, por ejemplo: jaqueo de contraseñas, ataques dirigidos por datos, explotación de bugs de software, ingeniería social, negociación de servicios, phishing, reenvió de paquetes, rubberhose, ransomware, snnifing, spoofing, troyanos, etc. Estos ataques son realizados por ciberterroristas, desarrolladores de virus, phreakers, script kiddie, crackers, atacantes internos; con disímiles motivos de extorsión.

Lo descrito anteriormente sugiere la necesidad de que el profesional en Ciencias de la Computación, especialmente el que estudia en la Universidad Politécnica Salesiana logre competencias de estudios de investigación, esto sumado al hecho de que la Universidad a pesar de tener equipos de hardware y bases estructurales idóneas, no cuenta con un LIF, que admita el desarrollo mediante seminarios que puedan recrear o analizar situaciones de trasgresiones informáticas que logren establecer una investigación forense digital y con esto cubrir las exigencias de l una sociedad.

Las organizaciones públicas y privadas eventualmente demandan el conocimiento, capacidades y habilidades al profesional de la carrera de Ciencias de la Computación para desarrollar una investigación forense dentro del marco legal regulatorio del país.

Justificación

El presente proyecto técnico busca proponer un modelo de implementación de un LIF que cuente con la infraestructura y herramientas forenses como hardware y software adecuados para realizar el trabajo de investigación digital dentro de los marcos legales que rigen en el país, de tal manera que el estudiante y docente adquieran el conocimiento para el debido proceso legal de un delito informático.

Actualmente el CPD de la carrera de Ciencias de la Computación cuenta con la infraestructura y equipos adecuados para la adecuación del Laboratorio de Informática Forense lo que permitirá a la carrera mantener un alto nivel de profesionalismo que demanda la sociedad ante el alto índice elevado de ataques informáticos ya que existen muy pocos profesionales con el conocimiento idóneo para este tipo de incidentes.

Un profesional de la carrera de Ciencias de la Computación de la Universidad Politécnica Salesiana puede alcanzar esta intuición y destreza para la administración y cosecha de evidencia, lo que accede que sus investigaciones sean conocidas como certeza de pruebas probatorias legales ante un juicio.

El trabajo de exploración en el LIF favorece a la ganancia de conocimiento, el mismo que puede ser injertado a través de los expertos de la sociedad mediante capacitaciones continuas.

El propósito del conocimiento que adquieran los estudiantes sobre el manejo de las técnicas de investigación forense digital es el de apoyar a detener y judicializar a los condenados de un hecho y describir las pruebas de cargo adecuadas que resulten en un veredicto condenatorio o en el caso contrario, absolver los cargos imputados.

Esta es una oportunidad para que la Universidad pueda implementar en su catálogo de servicios la investigación de informática forense.

Objetivo general

Desarrollar una propuesta para la implementación de un laboratorio de informática Forense dentro del Centro de Procesamiento de Datos de la Carrera de Ingeniería de Ciencias de la Computación de la Universidad Politécnica Salesiana, Sede Quito, Campus Sur.

Objetivos específicos

Adquirir conocimiento de las normativas legales ecuatorianas enfocadas en la informática forense para realizar una investigación debidamente sustentada en los marcos legales que rigen en el país.

Identificar el recurso humano, económico, infraestructura y tecnológico ineludibles para el delicado ejercicio del LIF propuesto.

Analizar la situación de la infraestructura y equipos que actualmente cuenta el CPD de la Carrera de Ciencias de la Computación, los mismos que se logran fructificar para el LIF.

Presentar una propuesta de investigación forense, debidamente documentada en donde se detalle cada una de las técnicas y herramientas a utilizar para cada tipo de delitos informáticos basado en la norma para la caracterización, colección, afirmación y conservación de evidencia digital (ISO 27037:2012).

Propuesta de Solución y Alcance

Este proyecto termina con la propuesta para la puesta en marcha, en que se determina las condiciones específicas para que el LIF funcione dentro de CPD, de la carrera de Ciencias de la Computación. Los elementos considerados para la realización de esta propuesta son:

- Detallar una distribución física que ablande la defensa de la información que se considere, además se debe salvaguardar la probidad de la evidencia.
- El laboratorio debe describir con una política de gestión de seguridad orientado en la ISO 27037:2012.
- Es esencial contar con el software de apoyo para las exploraciones a desarrollar y generar valores de hash, MD5, SHA-1 entre otros, del contenido que se alojan en las unidades de acopio custodiados.
- Es ineludible referir el hardware adecuado entre estos ordenadores forenses, Celldek, Ultrakit, Roadmasster, entre otros que consientan avalar la velocidad de procesamiento y la fiabilidad del contenido procesado.
- Plantear diferentes técnicas y sensibles prácticas que viven un apropiado examen de investigación forense digital.

La propuesta del laboratorio de informática Forense en la carrera de Ingeniería de Ciencias de la Computación, de la Universidad Politécnica Salesiana, sede Quito, campus Sur, quedará bajo la potestad de los directivos, para tomar la decisión de implementar el LIF.

Metodología

La metodología que se emplea en el presente proyecto es la investigación bibliográfica, ya que es la primera etapa del proceso investigativo que proporciona el

conocimiento de las investigaciones ya existentes de un modo sistemático a través de una amplia búsqueda de: información, conocimientos y técnicas sobre una cuestión determinada (Galarreta, 1994).

La investigación bibliográfica reúne la información de páginas web, artículos científicos y libros electrónicos al igual que propuestas similares al proyecto que se está planteando. Esto se considera un paso esencial en la investigación porque incluye un conjunto de criterios que abarcan la observación, la indagación, la interpretación, la reflexión y el análisis para obtener bases necesarias para el desarrollo de la investigación (Ayala, 2018). Las tareas básicas de una investigación bibliográfica son:

- Conocer y explorar todas las fuentes que puedan ser útiles.
- Leer todas las fuentes disponibles de modo discriminatorio, destacando los aspectos esenciales.
- Recaudación de los datos.
- Cotejar los datos obtenidos observando las coincidencias o discrepancias y evaluando su confiabilidad.
- Sacar las conclusiones correspondientes.

Lo antes mencionado determina la propuesta de implementación de un LIF en la Universidad Politécnica Salesiana, inspiración por el cual se efectúa la insurrección de los datos que se evalúa en los siguientes aspectos:

- Se estudia la legislación de delitos informáticos en el Ecuador.
- Calidad de la Informática forense.
- Instituir herramientas de hardware y software que gravitan a un LIF.

- Analizar la infraestructura y presupuesto requerido para la implementación.
- Antecedentes nacionales e internacionales de laboratorios creados.
- Habilidades necesarias para el personal que labore en el LIF.
- Documentar los procesos para la construcción de un LIF.

Por otra parte, se tiene la exploración proyectiva se sitúa a la explicación de temas académicos, institucionales, políticos y públicos. La causa metodológica posee avisos determinados de proyecciones especiales, accesibles, realizables y coherentes de ejercicio (Hurtado, Centro Internacional de Estudios Avanzados Sypal, 2015). En la Figura 1 se detalla la investigación proyectiva mediante un esquema.

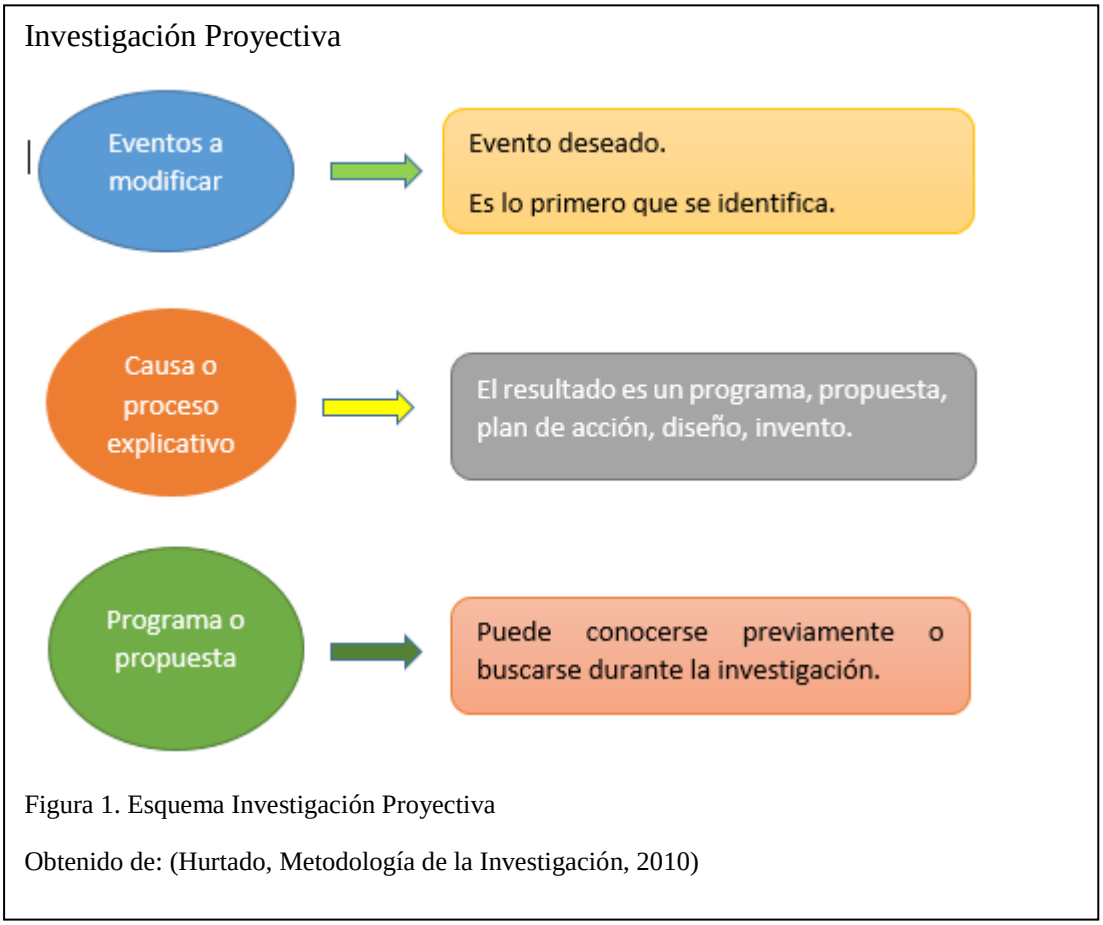

Figura 1. Esquema Investigación Proyectiva

Obtenido de: (Hurtado, Metodología de la Investigación, 2010)

Capítulo 1

1.1 Informática Forense

Mediante la comunicación a través de equipos, la información es expuesta a la maniobra de direcciones delictuosas que sobresalten a la probidad de nuestra sociedad. Con este tipo de inseguridades informáticas surge la necesidad de acudir a expertos para precautelar identidades, datos, dinero, reputación, propiedad intelectual entre otros aspectos.

El Buró Federal de Investigaciones (FBI) de los Estados Unidos de América, muestra que el procesamiento de datos es la técnica de espigar, conseguir, asegurar y exponer datos que han sido ejecutados y guardados electrónicamente dentro de unidades de acopio, El FBI es la entidad federal que encomienda perpetrar investigaciones de asaltos informáticos que atacan las redes de la sección pública o privado, las vitales embestidas se ejecutan a empresas, servicios corporativos, individuales, centros de educación, gobiernos y universidad que se encuentran en estudios de alto rendimiento, son entes focales hacia una arremetida, los individuos son atacadas por timadores, los niños por desequilibrados en línea. Todas las agresiones son ocasionadas por personas internas o externas a una nación (FBI, 2018).

2.1.1 Computación Forense (Computer Forensics)

El estudio de las Ciencias Forenses admite identificar, observar y aclarar los datos almacenados en los equipos informáticos y de este modo se atañen evidencias que formulen engreimientos correspondientes a los asuntos investigados.

1.1.2 Forensic en Redes (Network Forensics)

La investigación forense sobre redes implica los manejos de etiquetas, infraestructura, configuraciones de equipos de comunicación, los que permiten obtener un diagnostico específico sobre la conducta de movimientos extraños que afectan a la seguridad de la estructura funcional del negocio.

1.1.3 Forensia Digital (Digital Forensics)

El análisis forense digital es un conjunto de técnicas especializadas en recolectar información que permita examinar, documentar datos reales que sean acoplables durante un proceso judicial.

El artículo de (Octavio, 2017), indica que la Informática Forense se encarga de estudiar sistemas informáticos que aseguren la evidencia digital mediante herramientas de hardware y software que permitan la extracción de información relevante y real que sea comprobatoria dentro de una investigación.

1.2 Ciencias Forenses

El trabajo de (Mite Villón & Sanchez Montero, 2016), determina que: las saberes forenses consiguen especificar conjuntos de disciplinas, en el que el objetivo esencial es la percepción de pruebas para ser vinculado con una causa judicial, esto conlleva a encontrar los autores del suceso acontecido, salvaguardando la probidad y privacidad de los datos espigados mediante herramientas Open Source o modalidad de pago.

1.3 Antecedentes de delitos informáticos

Con crecimiento de la tecnología durante esta última década han crecido de igual manera los ataques informáticos que afectan a personas, pequeñas y grandes empresas, se considera que el 75% de los ataques son a sistemas informáticos que se ejecutan dentro de las organizaciones, lo que se hace vulnerable a pérdida de información que es utilizada a modo de extorsión o modalidad de desagravio.

Los ataques atañen a la indisponibilidad de sistemas computacionales que manejan gobiernos, empresas, sociedades e individuos lo que desgarra las reglas de seguridad que operan dentro de las instituciones, se ha tenido casos de agresiones de ingeniería social lo que accede a cumplir actos ilícitos en beneficio del atracador. Las violaciones informáticas son acciones ilegales que se glosan mediante técnicas computaciones. En agosto del 2014, fecha que entró en vigencia el Código Orgánico Integral Penal (COIP) en el Ecuador ciertos artículos se encargan de inspecciona y censurar las amenazas informáticas en referencia a el descubrimiento ilegal de base de datos, la apropiación ilegal de datos, traspaso electrónico de capital logrado de carácter ilegal, agresión a los de sistemas computacionales, direcciones no consentidos, obscenidad infantil, importunación sexual, los cuales son castigados con condena privativa de libertad de 1 a 3 años establecido en al Artículo 190 del COIP (Ecuador P. N., 2015).

El curso de Ciberseguridad de CISCO 2018, determina que: los atacantes son personas o grupos que pretenden fructificar las vulnerabilidades para conseguir una ganancia personal o financiera. Los agresores se interesan en las diferentes formas de lucrar (Academy, 2018).

1.4 Script Kiddies

Individuos con insuficiente pericia técnica e inmadurez, comúnmente manejan herramientas efectivas en internet para acarrear una embestida, los atacantes manipulan aplicaciones para instruirse, seguir la pista, averiguar, ensayar y hacer asaltos en los cuales manifiesta su habilidad y causa daños que pueden ser hostiles u perjudiciales que sobrelleven a términos judiciales (Gudiño, 2017).

1.5 Hackers

Personas que poseen un juicio muy amplio en sistemas computacionales que generalmente efectúan exploraciones a sistemas informáticos consintiendo de forma legal o ilegal para lograr ganancias y aumentar sus capacidades intelectuales, tienen técnicas de estudio que alcanzan a satisfacer su autoestima, el hacker tiene el mando de operar diferentes tipos de lenguajes de programación.

1.6 Tipos de delitos informáticos

Son actividades ilícitas, que se comete a través de medios y dispositivos tecnológicos y de comunicación, cuyo objetivo es causar algún daño, provocar pérdidas o impedir el uso de sistemas informáticos. En los últimos tiempos la pornografía infantil, fraudes informáticos e incluso actividades terroristas, han sido considerados como nuevos delitos informáticos.

1.6.1 Ciberacoso (**Cyberbullying**)

Es relacionado como una agresión que se cumple mediante las redes sociales, chat, foros, comunidades, blog, mensajería, juegos, servicios electrónicos, no siempre un acoso es físico sino digital manejando conjunto de técnicas de información, el propósito es embestir a los individuos que presente una baja autoestima, el agresor

concibe satisfacción cuando alcanza a establecer el ataque, lo que puede cristianizar en una intimidación o perjuicio que perturba de modo inmediato (Información, 2015).

1.6.2 Robo de identidad

La usurpación de identidad es una modalidad agresiva que utilizan los atacantes para conseguir datos públicos o privados de la víctima y de esta forma acceder a la información sin ser percibidos ante los sistemas de seguridad, estos ataques son propicios para delitos de extorsión, manipulación y modificación de información que asegure la confiabilidad del agresor.

1.6.3 Secuestro de datos (Ransomware)

Es un procedimiento que paraliza el acceso a cierto tipo de datos que se hallan residentes en discos, equipos informáticos generando inestabilidad, el objetivo vital de este malware es el pago inmediato que se cumple mediante transacciones, débitos automáticos, si la víctima no accede, la información capturada no es restituida por el atracador.

1.7 Principios básicos para el manejo de pruebas digitales

El trabajo de Francisca Rodríguez 2018, determina que: El trabajo denominado The High Tech Crimen, conocido como el Grupo de Lyon (U.S.A) – encargó a la IOCE (International Organization for Cooperation in Evaluation) es el proceso de una serie de elementos aplicables a las formas para la recolección de pruebas digitales, técnicas que garantizan la fiabilidad de las pruebas recolectadas (Rodríguez, 2018).

- Las pruebas recolectadas deben tener una metodología que proteja la información adquirida.
- La administración de las pruebas digitales se debe tratar con minuciosidad, cautela, seguridad y sobre todo debe estar documentada.
- Todo análisis que se realice sobre las pruebas digitales debe realizarse sobre imágenes y de esta manera se preserva la evidencia cruda.

Las instrucciones explicadas sobrellevan a una buena sistemática científica y documental en la extracción y estudio del contenido digital (Rodríguez, 2018).

1.8 Sustento de pruebas

De acuerdo al artículo de la página web sobre Evidencia Digital Colombia 2018, determina que: Una prueba digital es cualquier valor probatorio que debe ser tratada sin causar perjuicio y puede ser manejada ante un juicio penal, para tener un costo probatorio de acuerdo a la legislación vigente en cada país, la prueba puede ser admitida si el valor es sopesado frente a su naturaleza (Colombia, 2018).

Los procedimientos que se debe seguir son:

- No se debe desconectar los aparatos electrónicos para evitar perdida de contenido en las unidades de acopio.
- No se debe desconectar los terminales de la red, pues de esta forma se logra estudiar los accesos no acreditados.
- No abrir documentos, archivos dentro de los dispositivos afectados puede ocasionar alteraciones en la fecha y hora.
- No se debe ejecutar ningún tipo de programa dentro de los dispositivos afectados ya que se podría sobrescribir los datos a ser investigados.

El método de defender el contenido en su primitiva etapa es mediante el cerco electrónico de la escritura del dispositivo de arranque, de esta forma manipular los duplicados del contenido que se esgrimieran para efectuar los estudios de manera indudable y íntegra ante la investigación sin enredar la evidencia original (Colombia, 2018).

1.9 Delitos Informáticos en Ecuador

Las infracciones informáticas dentro del Ecuador han ido acrecentando gradualmente con el progreso de los procesos de la informática, actualizaciones en embestidas cibernéticos, los ciudadanos son objetivo primordial para efectuar una agresión, enredando la probidad de la información.

El Doctor Juan José Páez Rivadeneira planteo en el 2010 que el Código Penal Ecuatoriano en relación con infracciones cibernéticas muestran vacíos en cuanto a la exploración informática que se perpetra en el país (Rivadeneira, 2010).

1.10 La tipificación del delito informático en la Ley penal ecuatoriana

Durante el año 2009, el Ecuador empieza a sufrir delitos de informática forense, siendo así en el año 2103 se registra incidentes que bordean 3143 casos de infiltraciones, actualmente en el año 2019 el viceministro de Telecomunicaciones informa que el país ha sufrido más de 40 millones de ataques cibernéticos sobre denegación de servicios a páginas de instituciones gubernamentales, banco central, ministerios, zonas militares entre otras entidades públicas y privadas, los ataques han sido geo localizadas dentro y fuera del país, estas agresiones se han incrementado desde que el Ecuador decidió retirarle el asilo diplomático a Julian Assange,

fundador de WikiLeaks, el 11 de abril del 2019, quien residía en la Embajada de Ecuador en Londres (Universo, 2019).

Los violaciones informáticas se hallan plasmados en el artículo 190 del Código Orgánico Integral Penal que establece como delito "el uso de un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, es sancionada con pena privativa de libertad de uno a tres años" (Asamblea Nacional del Ecuador, 2014). Los delitos informáticos citados son los siguientes:

De acuerdo al Artículo 229.- *"Revelación ilegal de base de datos"***,** Conseguido del (Código Orgánico Integral Penal, 2014, página 36), menciona que el individuo que popularice información privada registrada en dispositivos electrónicos es sancionado con una penalidad de tres a cinco años (Asamblea Nacional del Ecuador, 2014).

En referencia al Artículo 230.- *"Interceptación ilegal de datos",* Obtenido del (Código Orgánico Integral Penal, 2014, página 36), indica la persona que guarde, visualice, escuche y utilice el contenido para desplegar programas que inciten a las personas aprobar sitios web diferentes a los que quieren acceder, es castigado con pena de tres a cinco años (Asamblea Nacional del Ecuador, 2014).

En referencia al Artículo 231.- *"Transferencia electrónica de activo patrimonial"*, Derivado del (Código Orgánico Integral Penal, 2014, página 37) - El individuo que trastorne los datos que contienen los sistemas informáticos para cumplir actos de

lucro sin consentimiento de la otra persona, es castigado con penalidad de libertad de tres a cinco años (Asamblea Nacional del Ecuador, 2014).

De acuerdo con el Artículo 232.- *"Ataque a la integridad de sistemas informáticos"*, Obtenido del (Código Orgánico Integral Penal, 2014, página 37), alude que la persona ejecute reformas o arruine sistemas informáticos físicos o lógicos, es condenado con pena de tres a cinco años (Asamblea Nacional del Ecuador, 2014).

En referencia al Artículo 233.- *"Delitos contra la información pública reservada legalmente"*, Obtenido (Código Orgánico Integral Penal, 2014, página 37), menciona que la persona que atente o enrede la protección de la información, es castigado con penalidad de siete a diez años (Asamblea Nacional del Ecuador, 2014).

De acuerdo al Artículo 234.- *"Acceso no consentido a un sistema informático, telemático o de telecomunicaciones"* Obtenido del (Código Orgánico Integral Penal, 2014, página 37), menciona que la persona que ingrese, manipule, elimine información de los sistemas computacionales sin consentimiento autorizado, es penalizado de tres a cinco años (Asamblea Nacional del Ecuador, 2014).

Según el Artículo 456.- *"Cadena de custodia"*, Obtenido (Código Orgánico Integral Penal, 2014, página 72), menciona que se brindará seguridad a las pruebas digitales salvaguardando el estado original y autenticidad para ser examinadas durante una investigación (Asamblea Nacional del Ecuador, 2014).

Según el Artículo 457.- *"Criterios de valoración"*, Obtenido de (Código Orgánico Integral Penal, 2014, página 72), enseña que las pruebas digitales son sometidas a una sucesión de protección científica y técnica, resguardando la legitimidad de la prueba real (Asamblea Nacional del Ecuador, 2014).

De acuerdo con el Artículo 500, sobre *"Contenido digital"*, Obtenido del (Código Orgánico Integral Penal, 2014, página 81), revela que el contenido es procesado bajo los estándares de preservación de datos, conservando la probidad de los datos hacer investigado bajo técnicas de estudios digitales (Asamblea Nacional del Ecuador, 2014).

1.11 ISO 27037:2012

El término evidencia digital de acuerdo con la ISO/IEC 27037 (2012), se conoce como *"información o datos, almacenados o transmitidos de forma binaria que pueden ser tomados en cuenta como evidencia o prueba"* (Normalización, 2012) ISO 27037:2012, encamina a la administración de las pruebas digitales, mediante la extracción, estudio y seguridad de los datos que consigue ser evidencia probatoria. Permite a las empresas facilitar procedimientos reglamentarios y disciplinarios que conserven la evidencia digital su objetivo es facilitar la usabilidad de la evidencia en distintas jurisdicciones por procesos legales (Normalización, 2012). ISO / IEC 27037:2012 suministra orientación para los siguientes dispositivos y circunstancias:

- Medios de acopio digital externos o internos
- Dispositivos móviles, tarjetas de memoria internas y externas
- Dispositivos de navegación por GPS
- Dispositivos de captura de imagen y video digital
- Computadoras conectadas a la red

Hay que aclarar que esta normativa no indica que herramientas se debe de utilizar, más bien, esta norma está claramente orientada a los procedimientos periciales de

evidencias digitales. Los pasos principales que indica esta normativa son los siguientes:

- Identificación
- Recolección
- Preservación
- Análisis y reporte de la evidencia
- Revisión

1.12 Criptografía

La Criptografía es una habilidad que se relaciona sobre el resguardo o el ocultamiento de la información frente a observadores no delegados, su apropiación, alteración o la introducción de información extra que también se puede aplicar al acceso no autorizado de los recursos de una red o sistema informático para prevenir denegación de los servicios a los sistemas las plataformas informáticas (DMA, 2018).

Capítulo 2

2.1 Antecedentes de la infraestructura inicial

Mediante información digital del inventario de hardware de los laboratorios de Servidores, CISCO, IHM (Interacción Humano Máquina), entregado por parte del personal de soporte del CPD, se procede a levantar el inventario de software de los laboratorios antes mencionados, de esta manera teniendo la información se puede determinar el uso de software y hardware para implementación en el laboratorio de informática forense.

2.2. Inventarios de Laboratorios de la Carrera de Computación

En el bloque D de la carrera de Computación de la Universidad Politécnica Salesiana, se encuentra ubicado 5 laboratorios:

- Laboratorio de Networking 1
- Laboratorio de Networking 2
- Laboratorio de Networking 3
- Laboratorio de Computación Avanzada
- Laboratorio IHM

Cada uno de estos laboratorios se encuentra bajo estándares de seguridad industrial que se compone en accesos mediante biométrico, cámaras de seguridad, puertas magnéticas, detectores de incendios, extintores y una central de energía que soporta a los laboratorios.

2.2.1 Laboratorio de Networking 1

El laboratorio se encuentra ubicado en el primer piso del bloque D, el cual dispone de 31 equipos modelo OPTIPLEX 7050 SFF i7-7700, con sistema operativo Windows 10 y máquinas virtuales en Ubuntu los cuales se detalla en la Tabla 1 y 2.

Tabla 1. Laboratorio Networking 1

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR	DATA CENTER DE LA CARRERA DE INGENIERIA DE SISTEMAS Y CIENCIAS DE LA COMPUTACIÓN														
	FORMATO	REGISTRO MAQUINAS LABORATORIO DE SERVIDORES													
				CPU		MONITOR			TECLADO			MOUSE			
ID	MODELO	SERIE	CODIGO UPS	EXPRESS SERVICE CODE	MIG.DATE	SERVICE TAG	EXPRESS SERVICE CODE	MIG.DATE	MODELO	CODIGO	MIG.DATE	MODELO	CODIGO	MIG.DATE	UBICACIÓN
LS-MAQPROF	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZ9VWK2	80042000617367	36961438610	20170811	1FLTYJ2	3120444686	CN-0Y01GT-QDC00-765-0HLU-A01	KB216P	CN-08NYJV-73826-747-02YN-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0HDK	2017-06	DOCENTE
LS-MAQ01	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZBSWK2	80042000617368	36964657874	20170811	GHLTYJ2	35893112078	CN-0Y01GT-QDC00-765-0K6U-A01	KB216P	CN-08NYJV-73826-747-00O0-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0GUM	2017-06	
LS-MAQ02	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZDVWK2	80042000617369	36968157074	20170811	3JLTYJ2	7715874062	CN-0Y01GT-QDC00-765-0KCU-A01	KB216P	CN-08NYJV-73826-747-030U-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0GWA	2017-06	
LS-MAQ03	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZ92JK2	80042000617370	36960068738	20170811	9DLTYJ2	20413771022	CN-0Y01GT-QDC00-765-0HCU-A01	KB216P	CN-08NYJV-73826-747-02YL-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0HAA	2017-06	
LS-MAQ04	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZCTWK2	80042000617371	36966184146	20170811	3HLTYJ2	7594941710	CN-0Y01GT-QDC00-765-0JTU-A01	KB216P	CN-08NYJV-73826-747-02ZW-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0GUW	2017-06	
LS-MAQ05	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZD2JK2	80042000617372	36966787202	20170811	4HLTYJ2	9771724046	CN-0Y01GT-QDC00-765-0JUU-A01	KB216P	CN-08NYJV-73826-747-00NZ-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0GV2	2017-06	FILA1
LS-MAQ06	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZB3JK2	80042000617373	36963474626	20170811	FFLTYJ2	33595397390	CN-0Y01GT-QDC00-765-0J2U-A01	KB216P	CN-08NYJV-73826-747-030Z-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0HKN	2017-06	
LS-MAQ07	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZD4JK2	80042000617374	36966880514	20170811	CFLTYJ2	27065050382	CN-0Y01GT-QDC00-765-0J0U-A01	KB216P	CN-08NYJV-73826-747-00OA-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0HS2	2017-06	
LS-MAQ08	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZCWWK2	80042000617375	36966524114	20170811	FDLTYJ2	33474465038	CN-0Y01GT-QDC00-765-0HGU-A01	KB216P	CN-08NYJV-73826-747-00O6-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0GUC	2017-06	
LS-MAQ09	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZ95JK2	80042000617376	36960208706	20170811	BFLTYJ2	24888268046	CN-0Y01GT-QDC00-765-0HYU-A01	KB216P	CN-08NYJV-73826-747-02YA-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0GXM	2017-06	
LS-MAQ10	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZC3JK2	80042000617377	36965154242	20170811	3GLTYJ2	7534475534	CN-0Y01GT-QDC00-765-0J8U-A01	KB216P	CN-08NYJV-73826-747-00NW-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0HU6	2017-06	
LS-MAQ11	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZCVWK2	80042000617378	36966477458	20170811	JGLTYJ2	42362992910	CN-0Y01GT-QDC00-765-0JNU-A01	KB216P	CN-08NYJV-73826-747-02YB-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0GTU	2017-06	
LS-MAQ12	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZCSWK2	80042000617379	36966337490	20170811	7GLTYJ2	16241604878	CN-0Y01GT-QDC00-765-0JDU-A01	KB216P	CN-08NYJV-73826-747-02ZH-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0GUF	2017-06	
LS-MAQ13	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZC4JK2	80042000617380	36965200898	20170811	6FLTYJ2	14004356366	CN-0Y01GT-QDC00-765-0HTU-A01	KB216P	CN-08NYJV-73826-747-030V-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0GWQ	2017-06	
LS-MAQ14	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZ9SWK2	80042000617381	36961298642	20170811	5HLTYJ2	11948506382	CN-0Y01GT-QDC00-765-0JVU-A01	KB216P	CN-08NYJV-73826-747-02YW-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0HPI	2017-06	
LS-MAQ15	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZ8TWK2	80042000617382	36959665682	20170811	BJLTYJ2	25130132750	CN-0Y01GT-QDC00-765-0KKU-A01	KB216P	CN-08NYJV-73826-747-018N-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0HRL	2017-06	
LS-MAQ16	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZC2JK2	80042000617383	36965107586	20170811	1GLTYJ2	3180910862	CN-0Y01GT-QDC00-765-0J6U-A01	KB216P	CN-08NYJV-73826-747-00O7-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0HU5	2017-06	FILA 2
LS-MAQ17	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZ8VWK2	80042000617384	36959758994	20170811	4KLTYJ2	9953122574	CN-0Y01GT-QDC00-765-0KYU-A01	KB216P	CN-08NYJV-73826-747-02ZI-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0GUG	2017-06	
LS-MAQ18	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZBWWK2	80042000617385	36964844498	20170811	HJLTYJ2	38190826766	CN-0Y01GT-QDC00-765-0KRU-A01	KB216P	CN-08NYJV-73826-747-00OC-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0HTL	2017-06	
LS-MAQ19	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZBVWK2	80042000617386	36964797842	20170811	GFLTYJ2	35772179726	CN-0Y01GT-QDC00-765-0J3U-A01	KB216P	CN-08NYJV-73826-747-00O3-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0GTS	2017-06	
LS-MAQ20	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZB4JK2	80042000617387	36963521282	20170811	DGLTYJ2	29302298894	CN-0Y01GT-QDC00-765-0JJU-A01	KB216P	CN-08NYJV-73826-747-02YY-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0HQQ	2017-06	
LS-MAQ21	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZBTWK2	80042000617388	36964704530	20170811	GDLTYJ2	35651247374	CN-0Y01GT-QDC00-765-0HHU-A01	KB216P	CN-08NYJV-73826-747-00SA-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-00MZ	2017-06	
LS-MAQ22	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZ9TWK2	80042000617389	36961345298	20170811	6JLTYJ2	14246221070	CN-0Y01GT-QDC00-765-0KFU-A01	KB216P	CN-08NYJV-73826-747-02YU-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0HLC	2017-06	
LS-MAQ23	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZDSWK2	80042000617390	36968017106	20170811	BDLTYJ2	24767335694	CN-0Y01GT-QDC00-765-0HDU-A01	KB216P	CN-08NYJV-73826-747-00O1-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0GRP	2017-06	
LS-MAQ24	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZ93JK2	80042000617391	36960115394	20170811	DDLTYJ2	29120900366	CN-0Y01GT-QDC00-765-0HFU-A01	KB216P	CN-08NYJV-73826-747-02ZY-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0GUX	2017-06	
LS-MAQ25	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZ94JK2	80042000617392	36960162050	20170811	DHLTYJ2	29362765070	CN-0Y01GT-QDC00-765-0K4U-A01	KB216P	CN-08NYJV-73826-747-02ZX-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0GVC	2017-06	FILA 3
LS-MAQ26	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZB2JK2	80042000617393	36963427970	20170811	7FLTYJ2	36014044430	CN-0Y01GT-QDC00-765-0KPU-A01	KB216P	CN-08NYJV-73826-747-02YE-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0HSE	2017-06	
LS-MAQ27	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZDTWK2	80042000617394	36968063762	20170811	GJLTYJ2	5297227022	CN-0Y01GT-QDC00-765-0HMU-A01	KB216P	CN-08NYJV-73826-747-030W-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0H27	2017-06	
LS-MAQ28	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZ9WWK2	80042000617395	36961485226	20170811	2FLTYJ2	20655635726	CN-0Y01GT-QDC00-765-0K1U-A01	KB216P	CN-08NYJV-73826-747-00VV-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0HB7	2017-06	
LS-MAQ29	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZD3JK2	80042000617396	36966833858	20170811	9HLTYJ2	14064822542	CN-0Y01GT-QDC00-765-0JCU-A01	KB216P	CN-08NYJV-73826-747-02ZZ-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0GTM	2017-06	
LS-MAQ30	COMPUTADOR OPTIPLEX 7050 SFF i7-7700 (CPU-MONITOR)	GZ8WWK2	80042000617397	36959805650	20170811	6GLTYJ2	16181138702	CN-0Y01GT-QDC00-765-0HUU-A01	KB216P	CN-08NYJV-73826-747-00NV-A02	Apr.2017	MS116p	CN-009NK2-73826-76H-0HT9	2017-06	

Nota: información obtenida de: CPD, 2019

Tabla 2. Inventario de Software Laboratorio de Networking 1

NOMBRE DEL PRODUCTO	MODELO DE VERSION	TAMAÑO	FABRICANTE	RESOLUCIÓN DE PANTALLA	LICENCIA
Ubuntu	18,04	7.7 GB 64BITS	Linux	1024 X 768	GPL
Eclipse	4.9 (Photon)	50.1MB	IBM	1024 X 768	Libre
Windows	10 PRO	10 GB	Microsoft	1024 X 768	Pagada
Arduino	1.8.7	182MB	Arduino	1024 X 768	GNU
VM Virtual Box	5.2.20	1,12 KB	Oracle	640 x 480	Libre
StarUML	V3.0.2	1,15 KB	MKLab	640 x 480	Software Libre
SQL Power Architect	3	2,5 KB	IBM	1024 X 768	GPL v.3
R x64	3.4.4	3 KB	Development Core Team	1024 X 768	GPL
MySQL	6,2	4GB	Oracle	1024X768	GPL
MatLab	9,1,0, 441655	4DB	Cleve Moler	1024X768	Propietaria
GNS 3	2.0.3	1,60 KB	Desarrolladores de GNS3	1024 X 768	GPLv3

Nota: información obtenida de: CPD, 2019

2.2.2 Laboratorio de Networking 2

El laboratorio se encuentra ubicado en el primer piso del bloque D, el cual dispone de 16 computadoras modelo OPTIPLEX 7060 MICRO XCT - 210-AOLK, con sistema operativo Windows 10 que se detalla en la Tabla 3 y 4.

Tabla 3. Inventario Laboratorio de Networking 2

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR				DATA CENTER DE LA CARRERA DE INGENIERIA DE SISTEMAS Y CIENCIAS DE LA COMPUTACIÓN				
				FORMATO	REGISTRO MÁQUINAS LABORATORIO DE NETWORKING 2			
ID	CPU			MONITOR		TECLADO	MOUSE	UBICACIÓN
	MODELO	SERIE	CODIGO UPS	MODELO	SERIE	MODELO	MODELO	
LN2-MAQPROF	Optiplex 9020	TF35CBY1	000171152499:45	DELL E1914HC		KB522	DELL S111-L	DOCENTE
LN2-MAQ01	OPTIPLEX 7060 MICRO XCT - 210-AOLK	CNNFBY1	80042000605313	DELL E1914HC	CN0R16JC7287237VA9HM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN2-MAQ02	OPTIPLEX 7060 MICRO XCT - 210-AOLK	CNQDSY1	80042000605312	DELL E1914HC	CNER'EJC7287237UAF9M	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN2-MAQ03	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F47DBY1	80042000605311	DELL E1914HC	CN0R16JC7287237VARKM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	FILA1
LN2-MAQ04	OPTIPLEX 7060 MICRO XCT - 210-AOLK	CNQCBY1	80042000605310	DELL E1914HC	CN0R16JC7287237OANAB	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN2-MAQ05	OPTIPLEX 7060 MICRO XCT - 210-AOLK	CNQCBY1	80042000605309	DELL E1914HC	CN0R16JC7287237VA8RM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN2-MAQ06	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F43FBY1	80042000605304	DELL E1914HC	CN0R16JC7287237VA98M	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN2-MAQ07	OPTIPLEX 7060 MICRO XCT - 210-AOLK	CN6DBY1	80042000605305	DELL E1914HC	CN0R16JC7287237VARFM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN2-MAQ08	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F42FBY1	80042000605307	DELL E1914HC	CN0R16JC7287237VALTM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	FILA 2
LN2-MAQ09	OPTIPLEX 7060 MICRO XCT - 210-AOLK	CP4FBY1	80042000605308	DELL E1914HC	CN0R16JC7287237OAP3B	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN2-MAQ10	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F38FBY1	80042000605306	DELL E1914HC	CN0R16JC7287237VA5KM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN2-MAQ11	OPTIPLEX 7060 MICRO XCT - 210-AOLK	TCN3DBY1	80042000605303	DELL E1914HC	CN0R16JC7287237VA58M	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN2-MAQ12	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F32DBY1	80042000605302	DELL E1914HC	CN0R16JC7287237VAP9M	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN2-MAQ13	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F50DBY1	80042000605309	DELL E1914HC	CN0R16JC7287237VA9MM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	FILA 3
LN2-MAQ14	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F48DBY1	80042000605301	DELL E1914HC	CN0R16JC7287237UAG2M	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN2-MAQ15	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F2ZFBY1	80042000605300	DELL E1914HC	CN0R16JC7287237UAFGM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	

Nota: información obtenida de: CPD, 2019

Tabla 4. Inventario de Software Laboratorio de Networking 2

NOMBRE DEL PRODUCTO	MODELO DE VERSION	TAMAÑO	FABRICANTE	RESOLUCIÓN DE PANTALLA	LICENCIA
Cisco Packet Tracer	7.1.1	4GB	CISCO	1024 X 768	Libre
Cisco Spark	WEBEX TEAMS	1.31 KB	CISCO	1024 X 768	Libre
Office Profecional 2016	1806 (Build 16.0.10228.20134)		Microsoft	1024 X 768	Trialware
Windows	10 PRO	10 GB	Microsoft	1024 X 768	Pagada
Wireshark	2.6.4	171 MB	Riverbed Technology	640 x 480	GPL
VM Virtual Box	5.2.20	1,12 KB	Oracle	640 x 480	Libre
GNS 3	2.0.3	1,60 KB	Desarrolladores de GNS3	1024 X 768	GPLv3
Cisco Aspire Networking Academy Edition	1.1.6.28 (CCNA Edition)	1GB	Cisco	1024 X 768	Libre

Nota: información obtenida de: CPD, 2019

Dentro del laboratorio de Networking 2 y Networking 3, se encuentra equipos de CISCO como se observa en la Tabla 5.

Tabla 5. Equipos de Networking

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR			DATA CENTER DE LA CARRERA DE INGENIERIA DE SISTEMAS Y CIENCIAS DE LA COMPUTACIÓN		
			FORMATO	EQUIPOS DE NETWORKING MAYO-2019	
N°	**EQUIPO**	**MODELO**	**MARCA**	**N° SERIE**	**UBICACIÓN**
1	Access Point	AIR-AP2802I-A-K9	CISCO	FJC2308M05S	Laboratorio Networking 2
2	Access Point	AIR-AP2802I-A-K9	CISCO	FJC2308M05M	Laboratorio Networking 2
3	Access Point	AIR-AP2802I-A-K9	CISCO	FJC2308M05N	Laboratorio Networking 2
4	Access Point	AIR-AP2802I-A-K9	CISCO	FJC2308M05Q	Laboratorio Networking 2
5	Access Point	AIR-AP2802I-A-K9	CISCO	FJC2308M05P	Laboratorio Networking 2
6	Access Point	AIR-AP2802I-A-K9	CISCO	FJC2308M05U	Laboratorio Networking 2
7	Wireless Controller	AIR-CT3504-K9	CISCO	FCW2307M02S	Laboratorio Networking 2
8	Wireless Controller	AIR-CT3504-K9	CISCO	FCW2305M126	Laboratorio Networking 2
9	Wireless Controller	AIR-CT3504-K9	CISCO	FCW2305M0Y8	Laboratorio Networking 2
10	Wireless Controller Rack Mount Tray	AIR-CT3504-RMNT	CISCO	S/N	Laboratorio Networking 2
11	Wireless Controller Rack Mount Tray	AIR-CT3504-RMNT	CISCO	S/N	Laboratorio Networking 2
12	Wireless Controller Rack Mount Tray	AIR-CT3504-RMNT	CISCO	S/N	Laboratorio Networking 2
13	Power Injector (802.3at) for Aironet Access Points	AIR-PWRINJ6	CISCO	C18206663000002986	Laboratorio Networking 2
14	Power Injector (802.3at) for Aironet Access Points	AIR-PWRINJ6	CISCO	C18206663000002889	Laboratorio Networking 2
15	Power Injector (802.3at) for Aironet Access Points	AIR-PWRINJ6	CISCO	C18206663000002853	Laboratorio Networking 2
16	Power Injector (802.3at) for Aironet Access Points	AIR-PWRINJ6	CISCO	C18196663000016568	Laboratorio Networking 2
17	Power Injector (802.3at) for Aironet Access Points	AIR-PWRINJ6	CISCO	C18206663000002842	Laboratorio Networking 2
18	Power Injector (802.3at) for Aironet Access Points	AIR-PWRINJ6	CISCO	C18206663000002893	Laboratorio Networking 2
19	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FOC2304Y3KD	Laboratorio Networking 2
20	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FCW2304A5TJ	Laboratorio Networking 2
21	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FCW2304A60G	Laboratorio Networking 2

22	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FOC2304Y3LG	Laboratorio Networking 2
23	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FOC2304Y3LM	Laboratorio Networking 2
24	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FOC2304Y3S7	Laboratorio Networking 2
25	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FCW2304A5ZA	Laboratorio Networking 2
26	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FOC2304Y3L5	Laboratorio Networking 2
27	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FOC2305Y04L	Laboratorio Networking 2
28	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FOC2304Y3MH	Laboratorio Networking 2
29	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FOC2304Y3F1	Laboratorio Networking 2
30	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FCW2304A60M	Laboratorio Networking 2
31	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FCW2304A5VS	Laboratorio Networking 2
32	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FCW2304Y3L3	Laboratorio Networking 2
33	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FCW2304A5P4	Laboratorio Networking 2
34	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FOC2304Y3LC	Laboratorio Networking 3
35	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FOC2304Y3DV	Laboratorio Networking 3
36	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FOC2305Y00L	Laboratorio Networking 3
37	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FOC2304Y3KW	Laboratorio Networking 3
38	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FOC2304Y3SW	Laboratorio Networking 3
39	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FCW2304A5VL	Laboratorio Networking 3
40	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FCW2304A5UN	Laboratorio Networking 3
41	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FOC2304Y3LX	Laboratorio Networking 3
42	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FOC2304Y3LS	Laboratorio Networking 3
43	Swicth Catalyst 2960	WS-C2960+24TC-L	CISCO	FCW2304A60H	Laboratorio Networking 3
44	Swicth Catalyst 2960 PLUS	WS-C2960+48TC-L	CISCO	FCW2245A09F	Laboratorio Networking 3
45	Swicth Catalyst 2960 PLUS	WS-C2960+48TC-L	CISCO	FCW2245A0H6	Laboratorio Networking 3
46	Swicth Catalyst 2960 PLUS	WS-C2960+48TC-L	CISCO	FCW2247A0JP	Laboratorio Networking 3
47	ASA	ASA5506-K9	CISCO	JMX2306G1MP	Laboratorio Networking 3
48	ASA	ASA5506-K9	CISCO	JMX2306G1MM	Laboratorio Networking 3
49	Swicth Catalyst 3650	WS-C3650-24TS-E	CISCO	FDO2235E2AG	Laboratorio Networking 3

50	Swicth Catalyst 3650	WS-C3650-24TS-E	CISCO	FDO2235E2AK	Laboratorio Networking 3
51	Swicth Catalyst 3650	WS-C3650-24TS-E	CISCO	FDO2235E2AD	Laboratorio Networking 3
52	Swicth Catalyst 3650	WS-C3650-24TS-E	CISCO	FDO2235E2A1	Laboratorio Networking 3
53	Swicth Catalyst 3650	WS-C3650-24TS-E	CISCO	FDO2235E2AH	Laboratorio Networking 3
54	Swicth Catalyst 3650 POE	WS-C3650-24PS-E	CISCO	FDO2251F09C	Laboratorio Networking 3
55	Swicth Catalyst 3650 POE	WS-C3650-24PS-E	CISCO	FDO2251F08M	Laboratorio Networking 3
56	Swicth Catalyst 3650 POE	WS-C3650-24PS-E	CISCO	FDO2251Q0EF	Laboratorio Networking 3
57	Swicth Catalyst 3650 POE	WS-C3650-24PS-E	CISCO	FDO2251F08K	Laboratorio Networking 3
58	Swicth Catalyst 3650 POE	WS-C3650-24PS-E	CISCO	FDO2251F08P	Laboratorio Networking 3
59	Router ISR 4221	ISR4221/K9	CISCO	FJC2308A07U	Laboratorio Networking 3
60	Router ISR 4221	ISR4221/K9	CISCO	FJC2308A07E	Laboratorio Networking 3
61	Router ISR 4221	ISR4221/K9	CISCO	FJC2308A07D	Laboratorio Networking 3
62	Router ISR 4221	ISR4221/K9	CISCO	FJC2308A07H	Laboratorio Networking 3
63	Router ISR 4221	ISR4221/K9	CISCO	FJC2308A07J	Laboratorio Networking 3
64	Router ISR 4221	ISR4221/K9	CISCO	FJC2308A07F	Laboratorio Networking 3
65	Router ISR 4221	ISR4221/K9	CISCO	FJC2308A07L	Laboratorio Networking 3
66	Router ISR 4221	ISR4221/K9	CISCO	FJC2308A07G	Laboratorio Networking 3
67	Router ISR 4221	ISR4221/K9	CISCO	FJC2308A07B	Laboratorio Networking 3
68	Router ISR 4221	ISR4221/K9	CISCO	FJC2308A07K	Laboratorio Networking 3
69	Router ISR 4221 SEC	ISR4221-SEC/K9	CISCO	FGL230812HG	Laboratorio Networking 3
70	Router ISR 4221 SEC	ISR4221-SEC/K9	CISCO	FGL230812HE	Laboratorio Networking 3
71	Router ISR 4221 SEC	ISR4221-SEC/K9	CISCO	FGL230812HH	Laboratorio Networking 3
72	Router ISR 4221 SEC	ISR4221-SEC/K9	CISCO	FGL230812HJ	Laboratorio Networking 3
73	Router ISR 4221 SEC	ISR4221-SEC/K9	CISCO	FGL230812HF	Laboratorio Networking 3
74	19 inch rack mount kit for Cisco ISR 4220	ACS-4220-RM-19	CISCO	S/N	Laboratorio Networking 3
75	19 inch rack mount kit for Cisco ISR 4220	ACS-4220-RM-19	CISCO	S/N	Laboratorio Networking 3
76	19 inch rack mount kit for Cisco ISR 4220	ACS-4220-RM-19	CISCO	S/N	Laboratorio Networking 3
77	19 inch rack mount kit for Cisco ISR 4220	ACS-4220-RM-19	CISCO	S/N	Laboratorio Networking 3

78	19 inch rack mount kit for Cisco ISR 4220	ACS-4220-RM-19	CISCO	S/N	Laboratorio Networking 3
79	19 inch rack mount kit for Cisco ISR 4220	ACS-4220-RM-19	CISCO	S/N	Laboratorio Networking 3
80	19 inch rack mount kit for Cisco ISR 4220	ACS-4220-RM-19	CISCO	S/N	Laboratorio Networking 3
81	19 inch rack mount kit for Cisco ISR 4220	ACS-4220-RM-19	CISCO	S/N	Laboratorio Networking 3
82	19 inch rack mount kit for Cisco ISR 4220	ACS-4220-RM-19	CISCO	S/N	Laboratorio Networking 3
83	19 inch rack mount kit for Cisco ISR 4220	ACS-4220-RM-19	CISCO	S/N	Laboratorio Networking 3
84	19 inch rack mount kit for Cisco ISR 4220	ACS-4220-RM-19	CISCO	S/N	Laboratorio Networking 3
85	19 inch rack mount kit for Cisco ISR 4220	ACS-4220-RM-19	CISCO	S/N	Laboratorio Networking 3
86	19 inch rack mount kit for Cisco ISR 4220	ACS-4220-RM-19	CISCO	S/N	Laboratorio Networking 3
87	19 inch rack mount kit for Cisco ISR 4220	ACS-4220-RM-19	CISCO	S/N	Laboratorio Networking 3
88	19 inch rack mount kit for Cisco ISR 4220	ACS-4220-RM-19	CISCO	S/N	Laboratorio Networking 3
89	2-Port Serial WAN Interface card	NIM-2T	CISCO	FOC23028XYZ	Laboratorio Networking 3
90	2-Port Serial WAN Interface card	NIM-2T	CISCO	FOC224939QJ	Laboratorio Networking 3
91	2-Port Serial WAN Interface card	NIM-2T	CISCO	FOC224939QM	Laboratorio Networking 3
92	2-Port Serial WAN Interface card	NIM-2T	CISCO	FOC224939PX	Laboratorio Networking 3
93	2-Port Serial WAN Interface card	NIM-2T	CISCO	FOC230369AQ	Laboratorio Networking 3
94	2-Port Serial WAN Interface card	NIM-2T	CISCO	FOC224939L2	Laboratorio Networking 3
95	2-Port Serial WAN Interface card	NIM-2T	CISCO	FOC224939LM	Laboratorio Networking 3
96	2-Port Serial WAN Interface card	NIM-2T	CISCO	FOC230369AV	Laboratorio Networking 3
97	2-Port Serial WAN Interface card	NIM-2T	CISCO	FOC23028Y55	Laboratorio Networking 3
98	2-Port Serial WAN Interface card	NIM-2T	CISCO	FOC23028Y4G	Laboratorio Networking 3
99	2-Port Serial WAN Interface card	NIM-2T	CISCO	FOC230369FH	Laboratorio Networking 3
100	2-Port Serial WAN Interface card	NIM-2T	CISCO	FOC224939R5	Laboratorio Networking 3
101	2-Port Serial WAN Interface card	NIM-2T	CISCO	FOC22493A3C	Laboratorio Networking 3
102	2-Port Serial WAN Interface card	NIM-2T	CISCO	FOC230369AN	Laboratorio Networking 3
103	2-Port Serial WAN Interface card	NIM-2T	CISCO	FOC22493A47	Laboratorio Networking 3
104	V.35 Cable, DCE Female to Smart Serial, 10 Feet	CAB-SS-V35FC	CISCO	S/N	Laboratorio Networking 3
105	V.35 Cable, DCE Female to Smart Serial, 10 Feet	CAB-SS-V35FC	CISCO	S/N	Laboratorio Networking 3

106	V.35 Cable, DCE Female to Smart Serial, 10 Feet	CAB-SS-V35FC	CISCO	S/N	Laboratorio Networking 3
107	CAB-SS-V35MT V.35 CABLE DTE MALE TO SMART SERIAL 10 FEET	CAB-SS-V35MT	CISCO	S/N	Laboratorio Networking 3
108	CAB-SS-V35MT V.35 CABLE DTE MALE TO SMART SERIAL 10 FEET	CAB-SS-V35MT	CISCO	S/N	Laboratorio Networking 3
109	CAB-SS-V35MT V.35 CABLE DTE MALE TO SMART SERIAL 10 FEET	CAB-SS-V35MT	CISCO	S/N	Laboratorio Networking 3

Nota: información obtenida de: CPD, 2019

2.2.3 Laboratorio de Networking 3

El laboratorio se encuentra ubicado en el primer piso del bloque D, el cual dispone de 16 computadoras modelo OPTIPLEX 7060 MICRO XCT - 210-AOLK, con sistema operativo Windows 10 que se detalla en la Tabla 6.

Tabla 6. Inventario Laboratorio de Networking 3

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR	DATA CENTER DE LA CARRERA DE INGENIERIA DE SISTEMAS Y CIENCIAS DE LA COMPUTACIÓN							
	FORMATO	*REGISTRO MAQUINAS LABORATORIO DE NETWORKING 3*						
ID	CPU			MONITOR		TECLADO	MOUSE	UBICACIÓN
	MODELO	SERIE	CODIGO UPS	MODELO	SERIE	MODELO	MODELO	
LN3-MAQPROF	Optiplex 9020	F3VDBY1	80042000605319	DELL E1912HF	CN0R16JC7287237VA8HM	KB522	DELL S111-L	DOCENTE
LN3-MAQ01	OPTIPLEX 7060 MICRO XCT - 210-AOLK	CN9FBY1	80042000605323	DELL E1912HF	CN0R16JC7287237VA5JM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN3-MAQ02	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F41FBY1	80042000605325	DELL E1912HF	CN0R16JC7287237OAPPB	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN3-MAQ03	OPTIPLEX 7060 MICRO XCT - 210-AOLK	CP0GBY1	80042000605328	DELL E1912HF	CN0R16JC7287237VAFVM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	FILA1
LN3-MAQ04	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F30GBY1	80042000605321	DELL E1912HF	CN0R16JC7287237UAG7M	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN3-MAQ05	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F34GBY1	80042000605324	DELL E1912HF	CN0R16JC7287237VA5GM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN3-MAQ06	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F30DBY1	80042000605326	DELL E1912HF	CN0R16JC7287237VA8KM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN3-MAQ07	OPTIPLEX 7060 MICRO XCT - 210-AOLK	CNTFBY1	80042000605327	DELL E1912HF	CN0R16JC7287237VA8TM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN3-MAQ08	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F40DBY1	80042000605320	DELL E1912HF	CN0R16JC7287237VARDM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	FILA 2
LN3-MAQ09	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F2XFBY1	80042000605322	DELL E1912HF	CN0R16JC7287237UAEHM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN3-MAQ10	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F2YDBY1	80042000605318	DELL E1912HF	CN0R16JC7287237UAFKM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN3-MAQ11	OPTIPLEX 7060 MICRO XCT - 210-AOLK	CNPGBY1	80042000605315	DELL E1912HF	CN0R16JC7287237VA5YM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN3-MAQ12	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F3ZFBY1	80042000605313	DELL E1912HF	CN0R16JC7287237UAE5M	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN3-MAQ13	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F2SDBY1	80042000605314	DELL E1912HF	CN0R16JC7287237UAFLM	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	FILA 3
LN3-MAQ14	OPTIPLEX 7060 MICRO XCT - 210-AOLK	F4GFBY1	80042000605316	DELL E1912HF	CN0R16JC7287237VAP2M	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	
LN3-MAQ15	OPTIPLEX 7060 MICRO XCT - 210-AOLK	CNPFBY1	80042000605317	DELL E1912HF	CN0R16JC7287237OANPB	Dell KB216 Wired Keyboard, Spanish 580-AECM	Black Dell MS116 Wired Mouse 275-BBBW	

Nota: información obtenida de: CPD, 2019

2.2.4 Laboratorio de Computación Avanzada

El laboratorio se encuentra ubicado en el primer piso del bloque D, el cual dispone de 19 computadoras modelo OPTIPLEX 9020, con sistema operativo Windows 10 que se detalla en la Tabla 7.

Tabla 7. Inventario Laboratorio de Computación Avanzada

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR	DATA CENTER DE LA CARRERA DE INGENIERIA DE SISTEMAS Y CIENCIAS DE LA COMPUTACIÓN								
	FORMATO	REGISTRO MÁQUINAS LABORATORIO COMPUTACIÓN AVANZADA							
ID	CPU			MONITOR			TECLADO	MOUSE	UBICACIÓN
	MODELO	SERIE	CODIGO UPS	MODELO	CODIGO UPS	SERIE	MODELO	MODELO	
LCA-MAQPROF	Optiplex 9020	3024942	80042000609175	DELL E1914HC	80042000609355	CN-04FF47-64180-4BU-O8KI	KB522	DELL S111-L	DOCENTE
LCA-MAQ01	Optiplex 9020	30H5942	80042000609183	DELL E1914HC	80042000609333	CN-04FF47-64180-4BS-1H3I	KB522	DELL S111-L	FILA1
LCA-MAQ02	Optiplex 9020	30N4942	80042000609178	DELL E1914HC	80042000609367	CN-04FF47-64180-4BS-12MI	KB522	DELL S111-L	
LCA-MAQ03	Optiplex 9020	2Y74942	80042000609166	DELL E1914HC	80042000609325	CN-04FF47-64180-4CD-2SKB	KB522	DELL S111-L	
LCA-MAQ04	Optiplex 9020	2Y63942	80042000609177	DELL E1914HC	80042000609342	CN-04FF47-64180-4BS-1GTI	KB522	DELL S111-L	
LCA-MAQ05	Optiplex 9020	3034942	80042000609179	DELL E1914HC	80042000609326	CN-04FF47-64180-4BS-12H1	KB522	DELL S111-L	
LCA-MAQ06	Optiplex 9020	2Z66942	80042000609176	DELL E1914HC	80042000609358	CN-04FF47-64180-4CD-2RQB	KB522	DELL S111-L	
LCA-MAQ07	Optiplex 9020	30S3942	80042000609174	DELL E1914HC	80042000609375	CN-04FF47-64180-4BS-1EYI	KB522	DELL S111-L	FILA 2
LCA-MAQ08	Optiplex 9020	2YG2942	80042000609172	DELL E1914HC	80042000609329	CN-04FF47-64180-4BS-135I	KB522	DELL S111-L	
LCA-MAQ09	Optiplex 9020	3047942	80042000609169	DELL E1914HC	80042000609328	CN-04FF47-64180-4BS-2QYI	KB522	DELL S111-L	
LCA-MAQ10	Optiplex 9020	30X5942	80042000609173	DELL E1914HC	80042000609335	CN-04FF47-64180-4CC-OF58	KB522	DELL S111-L	
LCA-MAQ11	Optiplex 9020	2Z67942	80042000609180	DELL E1914HC	80042000609334	CN-04FF47-64180-4BS-12SI	KB522	DELL S111-L	
LCA-MAQ12	Optiplex 9020	2Z37942	80042000609165	DELL E1914HC	80042000609341	CN-04FF47-64180-4BS-1ECI	KB522	DELL S111-L	
LCA-MAQ13	Optiplex 9020	2Y53942	80042000609171	DELL E1914HC	80042000609339	CN-04FF47-64180-4BS-1EKI	KB522	DELL S111-L	FILA 3
LCA-MAQ14	Optiplex 9020	2Z73942	80042000609168	DELL E1914HC	80042000609353	CN-04FF47-64180-4BS-114I	KB522	DELL S111-L	
LCA-MAQ15	Optiplex 9020	3004942	80042000609170	DELL E1914HC	80042000609372	CN-04FF47-64180-4BS-2PCI	KB522	DELL S111-L	
LCA-MAQ16	Optiplex 9020	2ZJ5942	80042000609167	DELL E1914HC	80042000609387	CN-04FF47-64180-4BU-09B1	KB522	DELL S111-L	
LCA-MAQ17	Optiplex 9020	31Z5942	80042000609164	DELL E1914HC	80042000609340	CN-04FF47-64180-4BU-123I	KB522	DELL S111-L	
LCA-MAQ18	Optiplex 9020	2Z65942	80042000609182	DELL E1914HC	80042000609343	CN-04FF47-64180-4BU-12QI	KB522	DELL S111-L	

Nota: información obtenida de: CPD, 2019

2.2.5 Laboratorio IHM (Interacción Humano Máquina)

El laboratorio se encuentra ubicado en el segundo piso del bloque D, el cual dispone de 31 computadoras modelo IMAC 21,5 4K Retina Core i5 Turbo Boost y sistema operativo IMAC, que se detalla en la Tablas 8 y 9.

Tabla 8. Inventario Laboratorio IHM

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR					DATA CENTER DE LA CARRERA DE INGENIERIA DE SISTEMAS Y CIENCIAS DE LA COMPUTACIÓN							
					FORMATO		*REGISTRO IMAC 21.5 4K RETINA CORE I5 TURBO BOOST*					
N°	IMAC				TECLADO		MOUSE		ACCESORIOS	REGISTRO		
	ID	MODELO	SERIE	CODIGO UPS	MODELO	SERIE	MODELO	SERIE	ESTUCHE	GRUPO	ICLOUD ACCOUNT	PASSWORD
1	LIHM_MAC01	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WC1YAJ1G5	´80042000619268	A1243	DG775121144DQY6AS	A1152	CC254360A2QDNYPA6	SI		dcicc.a.imac@gmail.com	Rimac*123
2	LIHM_MAC02	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WJ4KFJ1G5	´80042000619267	A1243	DG76330C4EDQY6A0	A1152	CC2543508L1DNYPAC	SI		dcicc.a.imac@gmail.com	Rimac*123
3	LIHM_MAC03	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WP02MJ1G5	´80042000619266	A1243	DG7710100Y2DQY6AT	A1152	CC25435071DDNYPAQ	SI		dcicc.a.imac@gmail.com	Rimac*123
4	LIHM_MAC04	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WP05NJ1G5	´80042000619265	A1243	DG764330C8JDQY6AP	A1152	CC25435071NDNYPAF	SI		dcicc.a.imac@gmail.com	Rimac*123
5	LIHM_MAC05	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WJ4KJJ1G5	´80042000619264	A1243	DG764540NGTDQY6A3	A1152	CC2543508N8DNYPAZ	SI		dcicc.a.imac@gmail.com	Rimac*123
6	LIHM_MAC06	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WP047J1G5	´80042000619270	A1243	DG7710100Y2DQY6AQ	A1152	CC254350747DNYPAM	SI	A	dcicc.a.imac@gmail.com	Rimac*123
7	LIHM_MAC07	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WD5GEJ1G5	´80042000619271	A1243	DG77101014JDQY6AF	A1152	CC25435073HDNYPAE	SI		dcicc.a.imac@gmail.com	Rimac*123
8	LIHM_MAC08	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WWP05SJ1G5	´80042000619172	A1243	DG7710100VSDQY6A9	A1152	CC254350743DNYPAR	SI		dcicc.a.imac@gmail.com	Rimac*123
9	LIHM_MAC09	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WJ4LHJ1G5	´80042000619273	A1243	DG764330D0UDQY6A2	A1152	CC2543508LGDNYPAX	SI		dcicc.a.imac@gmail.com	Rimac*123
10	LIHM_MAC10	Imac 21,5 4K Retina Core i5 Turbo Boost	C02W36WVJ1G5	´80042000619274	A1243	DG7710100QMDQY6AV	A1152	CC25435076GDNYPA6	SI		dcicc.a.imac@gmail.com	Rimac*123
11	LIHM_MAC11	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WD55AJ1G5	80042000619263	A1243	DG7710100WUDQY6A4	A1152	CC25435073YDNYPAZ	SI		dcicc.b.imac@gmail.com	Rimac*1234
12	LIHM_MAC12	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WJ4M1J1G5	80042000619262	A1243	DG7710100QRDQY6AR	A1152	CC2527305BTDNYPA8	SI		dcicc.b.imac@gmail.com	Rimac*1234
13	LIHM_MAC13	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WD5J4J1G5	80042000619261	A1243	DG77101012YDQY6AF	A1152	CC25435074RDNYPA3	SI		dcicc.b.imac@gmail.com	Rimac*1234
14	LIHM_MAC14	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WJ4KVJ1G5	80042000619260	A1243	DG7710101XHDQY6AB	A1152	CC2543508HQDNYPAY	SI		dcicc.b.imac@gmail.com	Rimac*1234
15	LIHM_MAC15	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WD5HEJ1G5	80042000619259	A1243	DG7710100RVDQY6AJ	A1152	CC2543508CNDNYPAF	SI		dcicc.b.imac@gmail.com	Rimac*1234
16	LIHM_MAC16	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WD5HGJ1G5	80042000619275	A1243	DG7710100Z2DQY6AM	A1152	CC2543508HBDNYPAB	SI	B	dcicc.b.imac@gmail.com	Rimac*1234
17	LIHM_MAC17	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WD5GWJ1G5	80042000619276	A1243	DG7710101RLDQY6A5	A1152	CC254350740DNYPAU	SI		dcicc.b.imac@gmail.com	Rimac*1234
18	LIHM_MAC18	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WP023J1G5	80042000619277	A1243	DG77101017KDQY6AD	A1152	CC2543508GDDNYPAC	SI		dcicc.b.imac@gmail.com	Rimac*1234
19	LIHM_MAC19	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WP04AJ1G5	80042000619278	A1243	DG771010121DQY6AC	A1152	CC25435072MDNYPAD	SI		dcicc.b.imac@gmail.com	Rimac*1234
20	LIHM_MAC20	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WD50WJ1G5	80042000619279	A1243	DG771010131DQY6A9	A1152	CC25435071FDNYPAN	SI		dcicc.b.imac@gmail.com	Rimac*1234
21	LIHM_MAC21	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WD00UJ1G5	80042000619258	A1243	DG7710100SADQY6A0	A1152	CC2543508MFDNYPAV	SI		dcicc.c.imac@gmail.com	Rimac*123
22	LIHM_MAC22	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WP02DJ1G5	80042000619257	A1243	DG771010259DQY6AU	A1152	CC2543508HCDNYPAA	SI		dcicc.c.imac@gmail.com	Rimac*123
23	LIHM_MAC23	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WH2P3J1G5	80042000619256	A1243	DG764330CQYDQY6AV	A1152	CC2535O8K4DNYPAC	SI		dcicc.c.imac@gmail.com	Rimac*123
24	LIHM_MAC24	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WD4X7J1G5	80042000619255	A1243	DG76433OCVNDQY6AQ	A1152	CC2543508LKDNYPAU	SI		dcicc.c.imac@gmail.com	Rimac*123
25	LIHM_MAC25	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WPO49J1G5	80092000619254	A1243	DG764330C55DQY6AG	A1152	CC25435073PDNYPA8	SI		dcicc.c.imac@gmail.com	Rimac*123
26	LIHM_MAC26	Imac 21,5 4K Retina Core i5 Turbo Boost	´C02WJ4M6J1G5	´80042000619280	A1243	DG764330CQSDQY6A1	A1152	CC2543508LEDNYPAZ	SI	C	dcicc.c.imac@gmail.com	Rimac*123
27	LIHM_MAC27	Imac 21,5 4K Retina Core i5 Turbo Boost	´C02WJ4M8J1G5	´80042000619281	A1243	DG764330CZBDQY6AP	A1152	CC2543508NZDNYPA8	SI		dcicc.c.imac@gmail.com	Rimac*123
28	LIHM_MAC28	Imac 21,5 4K Retina Core i5 Turbo Boost	´C02WD5HSJ1G5	´80042000619282	A1243	DG771010122DQY6AB	A1152	CC254460702DNYPA0	SI		dcicc.c.imac@gmail.com	Rimac*123
29	LIHM_MAC29	Imac 21,5 4K Retina Core i5 Turbo Boost	´C02WJ4M5J1G5	´80042000619283	A1243	DG7710100YGDQ6AA	A1152	CC2543508KWDNYPAL	SI		dcicc.c.imac@gmail.com	Rimac*123
30	LIHM_MAC30	Imac 21,5 4K Retina Core i5 Turbo Boost	´C02WJ4K8J1G5	´80042000619284	A1243	DG77101011CDQY6A4	A1152	CC25435075ADNYPAF	SI		dcicc.c.imac@gmail.com	Rimac*123
31	LIHM_MAC31	Imac 21,5 4K Retina Core i5 Turbo Boost	C02WPOSPJ1G5	´80042000619269	A1243	DG7710100X1DQY6AU	A1152	CC25435073SDNYPA5	SI	ADMINISTRACION		

Nota: información obtenida de: CPD, 2019

Tabla 9. Inventario Software IHM

NOMBRE DEL PRODUCTO	MODELO DE VERSION	TAMAÑO	FABRICANTE	RESOLUCIÓN DE PANTALLA	LICENCIA
IMAC	Retian 4L -inch 2017	8GB	Apple	1024 X 768	Propietaria
PgAdmin 4	11,1	4KB	PostgreSQL	1024 X 768	PostgreSQL License
Eclipse	4.9 (Photon)	4KB	IBM	1024 X 768	Libre
StarUML	V3.0.2	1,15 KB	MKLab	640 x 480	Software Comercial
Arduino	1.8.7	182MB	Arduino	1024 X 768	GNU

Nota: información obtenida de: CPD, 2019

Dentro del laboratorio de IHM, se tienen 13 Tablet con modelo GT-P5100, sistema operativo Android, visualice la información en la Tabla 10, adicional también se cuenta con 31 Ipad Mini 4 Wi-Fi 128 GB Space Grey, con sistema operativo IOS, observe la Tabla 11.

Tabla 10. Inventario Tabletas Android

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR					DATA CENTER DE LA CARRERA DE INGENIERIA DE			
					FORMATO	*REGISTRO TABLET ANDROID*		
N°	DESCRIPCION				ACCESORIOS			REGISTRO
	FC-ID	N° Anterior	MODELO	SERIE	TABLET	CABLE LIGTHNING	ADAPTADOR USB	GRUPO
1	A3LGTP5100	1	GT-P5100	RV1CA2YS3JN	SI	SI	SI	A
2	A3LGTP5100	14	GT-P5100	RV1CA34SR5P	SI	SI	SI	
3	A3LGTP5100	13	GT-P5100	RV1C97304WB	SI	SI	SI	
4	A3LGTP5100	5	GT-P5100	RV1CA0LNK1A	SI	SI	SI	
5	A3LGTP5100	20	GT-P5100	RV1CA2YS4HW	SI	SI	SI	
6	A3LGTP5100	3	GT-P5100	RV1CA2YSK4H	SI	SI	SI	
7	A3LGTP5100	2	GT-P5100	RV1CA0LNEWB	SI	SI	SI	
8	A3LGTP5100	15	GT-P5100	RV1CA2ZSQ2E	SI	SI	SI	
9	A3LGTP5100	9	GT-P5100	RV1CA0LNK5V	SI	SI	SI	
10	A3LGTP5100	11	GT-P5100	RV1CA34SFAW	SI	SI	SI	
11	A3LGTP5100	10	GT-P5100	RV1CA2YS44M	SI	SI	SI	
12	A3LGTP5100	12	GT-P5100	RV1CA2YS5JE	SI	SI	SI	
13	A3LGTP5100	4	GT-P5100	RV1AC2YT8SV	SI	SI	SI	

Nota: información obtenida de: CPD, 2019

Tabla 11. Inventario Tabletas Apple

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR	DATA CENTER DE LA CARRERA DE INGENIERIA DE SISTEMAS Y CIENCIAS DE LA COMPUTACIÓN								
	FORMATO					REGISTRO IPAD MINI 4			
N°	DESCRIPCION					ACCESORIOS			REGISTRO
	ID	NOMBRE	MODELO	SERIE	CODIGO UPS	IPAD MINI 4	CABLE LIGTHNING	ADAPTADOR USB	GRUPO
1	IPAD A DCICC	Ipad A1	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ88VGHKJ	'80042000619183	SI	SI	SI	A
2	IPAD A DCICC	Ipad A2	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ056GHKJ	'80042000619184	SI	SI	SI	
3	IPAD A DCICC	Ipad A3	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQCQZGHKJ	'80042000619185	SI	SI	SI	
4	IPAD A DCICC	Ipad A4	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ9YTGHKJ	'80042000619186	SI	SI	SI	
5	IPAD A DCICC	Ipad A5	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ9WSGHKJ	'80042000619187	SI	SI	SI	
6	IPAD A DCICC	Ipad A6	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ87HGHKJ	'80042000619188	SI	SI	SI	
7	IPAD A DCICC	Ipad A7	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ2SMGHKJ	'80042000619189	SI	SI	SI	
8	IPAD A DCICC	Ipad A8	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ8C4GHKJ	'80042000619190	SI	SI	SI	
9	IPAD A DCICC	Ipad A9	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ2N7GHKJ	'80042000619191	SI	SI	SI	
10	IPAD A DCICC	Ipad A10	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ80BGHKJ	'80042000619192	SI	SI	SI	
11	IPAD B DCICC	Ipad B1	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ2BJGHKJ	'80042000619193	SI	SI	SI	B
12	IPAD B DCICC	Ipad B2	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQB7SGHKJ	'80042000619194	SI	SI	SI	
13	IPAD B DCICC	Ipad B3	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ738GHKJ	'80042000619195	SI	SI	SI	
14	IPAD B DCICC	Ipad B4	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ9YDGHKJ	'80042000619196	SI	SI	SI	
15	IPAD B DCICC	Ipad B5	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ9YLGHKJ	'80042000619197	SI	SI	SI	
16	IPAD B DCICC	Ipad B6	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ7YXGHKJ	'80042000619198	SI	SI	SI	
17	IPAD B DCICC	Ipad B7	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWPERQGHKJ	'80042000619199	SI	SI	SI	
18	IPAD B DCICC	Ipad B8	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ0CEGHKJ	'80042000619200	SI	SI	SI	
19	IPAD B DCICC	Ipad B9	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ9XUGHKJ	'80042000619201	SI	SI	SI	
20	IPAD B DCICC	Ipad B10	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ7XCGHKJ	'80042000619202	SI	SI	SI	
21	IPAD C DCICC	Ipad C1	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQB9MGHKJ	'80042000619203	SI	SI	SI	C
22	IPAD C DCICC	Ipad C2	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ2QJGHKJ	'80042000619204	SI	SI	SI	
23	IPAD C DCICC	Ipad C3	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ85CGHKJ	'80042000619205	SI	SI	SI	
24	IPAD C DCICC	Ipad C4	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ03RGHKJ	'80042000619206	SI	SI	SI	
25	IPAD C DCICC	Ipad C5	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQB0AGHKJ	'80042000619207	SI	SI	SI	
26	IPAD C DCICC	Ipad C6	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ728GHKJ	'80042000619208	SI	SI	SI	
27	IPAD C DCICC	Ipad C7	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ2NNGHKJ	'80042000619209	SI	SI	SI	
28	IPAD C DCICC	Ipad C8	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ2QFGHKJ	'80042000619210	SI	SI	SI	
29	IPAD C DCICC	Ipad C9	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQCPCGHKJ	'80042000619211	SI	SI	SI	
30	IPAD C DCICC	Ipad C10	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQ2MVGHKJI	'80042000619212	SI	SI	SI	
31	IPad Master	Ipad Master	Ipad Mini 4 Wi-Fi 128 GB Space Grey	F9FWQB4YGHKJ	'80042000619213	SI	SI	SI	ADMINISTRACION

Nota: información obtenida de: CPD, 2019

Los equipos APOLLO 6000 HPE, STORAGE, SWITCH se encuentran dentro de DATA CENTER, ubicado en el segundo piso del bloque D, como se observa en la Tabla 12, 13 y 14.

Tabla 12. Registro de servidores APOLLO 6000 HPE

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR		DATA CENTER DE LA CARRERA DE INGENIERIA DE SISTEMAS Y CIENCIAS DE LA COMPUTACIÓN							
		FORMATO		REGISTRO SERVIDORES APOLLO 6000 HPE					
Servidor		HPE Apollo 1		HPE Apollo 2		HPE Apollo 3		HPE Apollo 4+GPU	
Modelo	HP Apollo	Serial N°	2M274600VG	Serial N°	2M274600VH	Serial N°	2M274600VJ	Serial N°	2M274600VK
Serial N	2M274600VL	Product N	789917-B21	Product N	789917-B21	Product N	789917-B21	Product N	768535-B21
Codigo UPS	80042000617365	Product Name	ProLiant XL230a Gen9	Product Name	ProLiant XL230a Gen9	Product Name	ProLiant XL230a Gen9	Product Name	ProLiant XL250a Gen9
Product N	735131-B21	ILO Default Network Settings		ILO Default Network Settings		ILO Default Network Settings		ILO Default Network Settings	
Storage HPE		Serial Number	2M274600VG	Serial Number	2M274600VH	Serial Number	2M274600VJ	Serial Number	2M274600VK
Modelo	3PAR 8200	User Name	Administrator	User Name	Administrator	User Name	Administrator	User Name	Administrator
Serial N	2M27320157	DNS Name	ILO2M274600VG	DNS Name	ILO2M274600VH	DNS Name	ILO2M274600VJ	DNS Name	ILO2M274600VK
Product N	K2Q36B	Password	RMPIVHWM	Password	LPWORAWR	Password	BOSEQBUL	Password	OEJDGLUD
		Discos Duros		Discos Duros		Discos Duros		Discos Duros	
		Tipo	Sas	Tipo	Sas	Tipo	Sas	Tipo	Sas
		Modelo	781577	Modelo	781577	Modelo	781577	Modelo	781577
		Capacidad	600 GB	Capacidad	600 GB	Capacidad	600 GB	Capacidad	600 GB
		N° Unidades	2	N° Unidades	2	N° Unidades	2	N° Unidades	2
		Transferencia	10k	Transferencia	10k	Transferencia	10k	Transferencia	10k

Nota: Recuperado del Inventario del Centro de Procesamiento de Datos, 2019.

Tabla 13. Registro de STORAGE 3PAR 8200

		DATA CENTER DE LA CARRERA DE INGENIERIA DE SISTEMAS Y CIENCIAS DE LA COMPUTACIÓN			
		FORMATO	*REGISTRO STORAGE 3PAR 8200*		
UNIDAD DE ALMACENAMIENTO		**Discos SAS**			
Modelo	3PAR Storage 8200	Modelo	N° de Discos	Capacidad por disco	Tipo de disco
Serie	EEAUBA2TF7429Y	3PAR 8000-844283	10	400 GB	MLC
HPE Part Number	QR490-63007	**Discos Normales**			
Replace with	756484-001	Modelo	N° de Discos	Capacidad por disco	Tipo de disco
Código UPS	8.0042E+13	3PAR 8000-840459	14	1.2 TB	10k

Nota: Recuperado del Inventario del Centro de Procesamiento de Datos, 2019.

Tabla 14. Registro de SWITCH SAN

		DATA CENTER DE LA CARRERA DE INGENIERIA DE SISTEMAS Y CIENCIAS DE LA COMPUTACIÓN	
SWITCH SAN 1 - ESPACIO 38		**SWITCH SAN 2 - ESPACIO 36**	
Modelo:	HPE SN3000B 24/12 FC Switch	Modelo:	HPE SN3000B 24/12 FC Switch
HPE P/N	QW937A	HPE P/N	QW937A
S/N	USB7282019	S/N	USB728202E
Código UPS	8.0042E+13	Código UPS	8.0042E+13
Revisión	0G	Revisión	0G
Replace With Spare	684428-001	Replace With Spare	684428-001
Código de Barras 1	CCD4028N02H	Código de Barras 1	CCD4028N03P
Código de Barras 2	HP-6505-12-0R-80-1006124-06	Código de Barras 2	HP-6505-12-0R-80-1006124-06

Nota: Recuperado del Inventario del Centro de Procesamiento de Datos, 2019.

2.2.5.1 Radio Comunicadores

Los equipos se encuentran en el laboratorio de IHM, a continuación, la información detallada en la Tabla 15.

Tabla 15. Radio de 2 vías

RADIO DE 2 VIAS		
Marca	MOTOROLA SOLUTIONS	MOTOROLA SOLUTIONS
Modelo	TALKABOUT T600 H2O	TALKABOUT T600 H2O
S/N	1754TA3081	1754TA3447
Cantidad	2	2

Nota: Recuperado del Inventario del Centro de Procesamiento de Datos, 2019.

2.2.5.2 Monitores

Los equipos se encuentran en el laboratorio de IHM, a continuación, la información detallada en la Tabla 16.

Tabla 16. Monitor 49INC LH49PMHP Series EDGE-LIT LED

MONITOR - UBICACIÓN NOC		
Descripción	Monitor 49INC LH49PMHP Series EDGE-LIT LED	Monitor 49INC LH49PMHP Series EDGE-LIT LED
Marca	Samsung	Samsung
Código UPS	80042000617628	80042000617629
Serie	06S2HCSJB01918A	0652HCJB019199K

Nota: Recuperado del Inventario del Centro de Procesamiento de Datos, 2019.

2.2.5.3 Televisores

Los equipos se encuentran en el laboratorio de IHM, a continuación, la información detallada en la Tabla 17.

Tabla 17. Televisor LED 4K

TELEVISOR - UBICACIÓN LABORATORIO SISTEMAS EMBEBIDOS		
Descripción	Televisor LED 4K UN-40MU6103G	Televisor LED 4K UN-40MU6103G
Marca	Samsung	Samsung
Código UPS	80042000617624	80042000617625
Serie	06YP3CFJA00727	06YP3CFJA00862

Nota: Recuperado del Inventario del Centro de Procesamiento de Datos, 2019.

2.2.5.4 Impresora

El equipo se encuentra en el laboratorio de IHM, a continuación, la información detallada en la Tabla 18.

Tabla 18. Impresora L575

IMPRESORA	
Descripción	Impresora L575 multifunción Tinta continua
Marca	Epson
Código UPS	80042000617637
Serie	W98Y190439

Nota: Recuperado del Inventario del Centro de procesamiento de Datos, 2019.

2.3 Laboratorio de Informática Forense UPS

Con la información que se tiene de la infraestructura de software y hardware de los laboratorios que se encuentran en el bloque D, de la Carrera de Computación, se puede realizar la implementación de un Laboratorio de Informática Forense en IHM (Laboratorio de Interfaz Humano Máquina), ya que cuenta con las respectivas seguridades y estándares basados ANSI/TIA-942, con las mejores características de redundancia, disponibilidad y seguridad que preserven la evidencia digital.

En este laboratorio se encuentran 31 equipos IMAC, que permiten realizar investigación de análisis de ingeniería social, estudio de imágenes a través de metadatos, recuperación de archivos, entre otros y de esta manera aprovechar al 100% las características que poseen estos equipos.

Para las investigaciones que se ejecuten en el laboratorio IHM, se puede realizar a través de Infraestructura de escritorio virtual (VDI) para conectarse a máquinas virtuales que contengan sistemas operativos Windows 10, para efectuar prácticas relacionadas a denegación de servicios, creaciones de imágenes, análisis de información que contiene la PC, análisis de logs, análisis de imágenes entre otros análisis relacionados a investigación forense digital.

Mediante la utilización de máquinas virtuales es necesario tener un sistema operativo de KALI – LINUX con versión 4.19.28 de 64 bits, esta herramienta fue diseñada

para cumplir auditorías de seguridad informática, lo que permite realizar investigaciones y análisis de memorias RAM, extracción de información multimedia eliminada de la aplicación WhatsApp en sistemas operativos Android, el IHM cuenta con 13 tablets modelo GT-P5100, para realizar este tipo de prácticas y otras que se realizan mediante KALI –LINUX.

En síntesis, el laboratorio de IHM cuenta con la infraestructura necesaria para la implementación del Laboratorio de Informática Forense.

El LIF debe contar con profesionales técnicos, ingenieros afines a área informáticas que sean competentes de sugerir, extraer pruebas, resguardarlas, indagar y mostrar manejando metodologías digitales forenses, así como elaborar informes legales que sean tomados como evidencias probatorias ante un juez.

Capítulo 3

3.1 Consideraciones generales para la implementación

La implementación de un LIF envuelve reconocer que los datos entregados por el cliente sean resguardados de modo seguro y confidencial. En el laboratorio se puede emplear formas para recolectar la evidencia como copia de seguridad del archivo crudo que puede ser enviado a un servidor ubicado físicamente en un laboratorio para que sea analizado y estudiado.

3.2 Prácticas de investigación y análisis forense para el laboratorio de la Carrera de Computación

Dentro de este plan se traza las prácticas que consiguen ejecutar estudios de investigación sobre agresiones cibernéticas utilizando herramientas de uso libre o mediante costos de licenciamiento.

3.2.1 Identificación de la ubicación de un ataque Phishing a través de un correo electrónico

Se busca asemejar la geolocalización de la IP pública de una ofensiva elaborado a una persona mediante un correo de Phishing, manejando la herramienta web Grabity IP Logger, para la reproducción del ataque y posterior examinar el mismo con la herramienta web Trace Email, donde se entrega la IP del origen del atacante.

3.2.1.1 Phishing

El Phishing hoy en día es una de las principales amenazas que se tiene en los ataques a través del e-mail o cualquier medio de comunicación. Los agresores tratan de que sus infiltraciones lleguen a tener éxito a un 100% de los Logs enviados mediante correo electrónico (Jiménez, 2018).

Los correos electrónicos de Phishing son fáciles de implementar, no se requiere de una gran preparación del agresor más allá de la elaboración de un correo que sea convincente y pueda captar la atención de la víctima. La mayor parte de correos no logra entrar a la bandeja de entrada, los ciberdelincuentes afinan sus técnicas de embestidas, lo que paraliza que la penetración sea más difícil de descubrir con los recursos de seguridad tradicionales (Jiménez, 2018).

El mensaje electrónico que se remite a la víctima rodea un enlace de Phishing que al inscribir el usuario y contraseña este logre aprisionar la información digitada por el beneficiario lo que consigue poseer mayor posibilidad de éxito ante el asalto ejecutado.

3.2.1.2 Dirección IP Pública y geolocalización

La IP pública es una dirección que administra el DHCP del router doméstico o comercial, que se recoge del distribuidor de servicio de internet (ISP), las terminales que se enlazan al internet mantienen IP’s únicas que acceden a una comunicación de origen y destino (Rivas, 2018).

El estudio de la geolocalización se basa en trata de situar la dirección geográfica de una dirección IP Pública, esto reside en determinar a una dirección IP una lugar geográfico, que tiene asociado un país de procedencia, región o estado, una ciudad e incluso información más detallada esto puede sujetar coordenadas pertenecientes a localización GPS entre ellas longitud y latitud (Ruiz, 2017).

Existen algunas empresas especializadas alrededor del mundo encargadas de entregar los dominios a las cuales pertenecen las IP´s a nivel mundial y de esta manera entregar la geolocalización que se almacenada en base de datos (Ruiz, 2017).

Se ejecuta la geolocalización de la IP pública de un ataque realizado a un sujeto que se envió un correo de Phishing, se maneja la herramienta web Grabity IP Logger para la reproducción del asalto y luego estudiar dicha ofensiva con la herramienta web Trace Email donde se indica la IP origen del ataque.

En los ataques Phishing se tiene varias técnicas que se utilizan para engañar a un usuario para obtener su confianza, esto con el fin de conseguir información personal. A pesar de acomodar herramientas que consiguen evitar ser víctimas de estas ofensivas, la mejor protección contra el Phishing comienza del propio usuario. Es preciso que el usuario tenga conocimiento de los riesgos y los métodos de Phishing con esto la persona puede asemejar de mejor manera cuando este en estos ataques.

La información emanada del estudio de un mensaje electrónico puede embutir en el conjunto de experimentos del delito que se está investigando, esto en un informe que proporcione el entendimiento del contenido técnico para los peritos.

Para un rastreo de una IP hay que efectuar una exploración mediante WHOIS, después hay que requerir la data al ISP (autorización legal), puede existir varios dispositivos acoplados en el mismo momento y cada equipo consigue tener más de un usuario inscrito en el sistema; luego de esto se debe establecer una serie de registros de la actividad para identificar los dispositivos y usuarios que operaron en cada momento.

Al momento de enviar un correo hay que realizar varias pruebas de ataque a diferentes usuarios para poder identificar y analizar varios escenarios en cuanto a proveedores de Correo electrónico; Hotmail, Gmail, Outlook, Yahoo!, ya que la estructura lógica de un correo no es la misma para los diferentes proveedores de correo electrónico como se observa anteriormente.

El procedimiento para poder identificar la localización de un ataque Phishing mediante un correo electrónico se la realiza en la práctica N° 1 que se describe a continuación.

3.2.1.3 Título de la práctica

Análisis de Phishing mediante un correo electrónico utilizando herramientas web Grabity IP Logger.

3.2.1.3.1 Objetivo general

Identificar la geolocalización de la IP pública de un ataque realizado mediante correo electrónico, utilizando la herramienta web Grabity IP Logger y determinar el ataque con la herramienta web Trace Email, la misma que entrega la dirección IP del origen de la infiltración.

3.2.1.3.2 Objetivos específicos

- Efectuar un simulacro de la ofensiva de Phishing mediante aplicaciones web para conseguir la IP pública de una compañía o individuo que se está siendo atacado.
- Examinar el encabezado que forma parte de los mensajes electrónicos, para hallar la IP del atacante.
- Luego de obtener la IP pública del origen del ataque se procederá a realizar la geolocalización utilizando la aplicación Web GEO IP.

3.2.1.3.3 Actividades por desarrollar

Para realizar el ataque de Phishing y analizar el correo enviado se debe utilizar los siguientes links de acceso:

- Atacante mediante Phishing: https://grabify.link/expander
- Hallar el del mensaje electrónico: https://whatismyipaddress.com/trace-email
- Ver Geolocalización de la dirección IP: https://es.geoipview.com
- Obtener el enlace clonado y capturar la dirección IP, se trabaja con el correo que se envía para conseguir la atención del mártir al cual se va a efectuar el ataque.

3.2.1.3.4 Resultados obtenidos

Se cumple la estructuración de un ataque de Phishing y el estudio de mensaje electrónico enviado para la agresión, el estudiante tiene la cabida de examinar, explorar, identificar e investigar los causales que tienen las agresiones realizadas mediante ingeniería social Phishing y determinar la realidad digital que encamine a encontrar al posible atacante.

En la parte de anexos se encuentra la práctica 1, donde se describe paso a paso cada una de las actividades, incluyendo procedimientos, conclusiones, recomendaciones y bibliografía.

3.2.2 Análisis de imágenes digitales mediante herramienta WEB FOTOFORENSICS

El estudio de imágenes fotográficas es muy utilizado ya que consiente acceder a la originalidad y naturalidad del objeto detallado, lo que se iguala a las características

de la imagen entre estos tiempos de creación, modificación de la reproducción analizada (ESET, 2019).

Con el crecimiento de la tecnología incrementa el uso de cámaras digitales que contengan capacidad de captura de retratos en tiempos reales jugando un papel importante con los metadatos de los lentes y sensores de las cámaras digitales, el desarrollo de maniobra de imágenes mediante aplicaciones que manejan los metadatos y afecta al usuario final, el objetivo de la práctica es garantizar que la imagen digital sea verídica ante un juicio (ESET, 2019).

Hoy en día existen diversas aplicaciones que permiten realizar modificaciones a las imágenes muy elaboradas que obstaculizan realizar la identificación de rasgos únicos que poseen las imágenes crudas, aunque es un análisis elemental es muy probable que se hayan alterado los metadatos (WELIVESECURITY, 2016).

Se identifica el origen y legitimidad de un retrato mediante una herramienta open-source Fotoforensics y se valida alteraciones sobre las fotografías analizadas mediante metadatos que conforma la imagen y los tipos de formatos de estas.

Hoy en día es muy habitual la edición de fotografías ya sea por una herramienta especializada o un filtro aplicado mediante una aplicación de fotografía es, por todo esto que hoy en día se complica saber si una fotografía es completamente original o es el resultado de una aplicación de edición o filtros de fotografía, es por lo que ahora existen diferentes herramientas que permiten identificar este tipo de cambios.

El análisis computacional de fotografías digitales es un escenario importante para comprobar el origen y la legitimidad de una imagen, para luego relacionarla a un individuo con una terminal, lugar o suceso. Por lo que los desafíos que afronta el técnico consisten en comprobar el origen de la fotografía, reconocer la marca,

modelo y terminal específico manipulado para tomar la fotografía y determinar si se ha introducido, suprimido o se ha realizado una modificación en la fotografía digital.

La herramienta que se utiliza admite los siguientes formatos: **jpeg, png** y webP. Esto es por un tema de espacio y procesamiento. Una imagen que se encuentra demasiado comprimida es difícil de identificar, por lo que el archivo que se analiza debe tener entre 100 x 100 px y 10000 x 10000 px.

Los metadatos en las imágenes requieren un análisis para confirmar los datos que se necesita para justificar la evidencia de que se realizó una alteración en la imagen. Estos datos son altamente sensibles al cambio, por esto es necesario ejecutar un duplicado de seguridad de la fotografía original para todos los análisis que se realice.

El procedimiento para poder Análisis de imágenes digitales mediante herramienta WEB FOTOFORENSICS se la realiza en la práctica N°2 que se describe a continuación.

3.2.2.1 Título de la práctica

Análisis de imágenes digitales mediante herramienta WEB FOTOFORENSICS.

3.2.2.1.1 Objetivo general

Identificar el origen, autenticidad a través de la herramienta open-source Fotoforensics y validar alteraciones sobre las imágenes analizadas mediante metadatos y tipos de formatos que conforma la imagen.

3.2.2.1.2 Objetivos específicos

- Determinar el origen, características y autenticidad de una fotografía, mediante los formatos que muestra la herramienta fotoforensics y de esta manera identificar alteraciones sobre la imagen analizada.
- Definir los elementos de la imagen como distribuciones, composición de línea, formas geométricas, colores dominantes, tonalidades y pixelaciones de una fotografía.

3.2.2.1.3 Actividades por desarrollar

- Es importante que los estudiantes realicen un énfasis en ataques mediante fotografías digitales que amedrente al usuario final, poniendo en duda su integridad personal.
- Para el reconocimiento de modificaciones en las imágenes es importante que la fotografía sea original, es decir obtenerla del dispositivo de la cual fue capturada para no perder información relevante que se desee analizar.
- La mayor cantidad de modificaciones no es visible al ojo humado lo que permite que se vulnerado, por este tipo de agresiones se utiliza Fotoforensics para identificar cambios no visibles hechos en imágenes.

Para realizar esta práctica se necesita utilizar el siguiente enlace de acceso:

Análisis de fotografías: http://fotoforensics.com/

3.2.2.1.4 Resultados obtenidos

Se observa que las imágenes analizadas en estado natural y editadas cambian sus tipos de archivo, tonalidades de grises. Focalización las misma que no son visibles al ojo humando, de esta manera se apoya con herramientas de análisis de ELA–

METADATOS, que determina y extrae la información relevante para el estudio de las características que poseen las fotografías.

En la parte de anexos se encuentra la práctica 2, donde se describe paso a paso cada una de las actividades, incluyendo procedimientos, conclusiones, recomendaciones y bibliografía.

3.2.3 Denegación de Servicios utilizando la herramienta HOIC

La evolución de la tecnología e internet se ha acelerado a maneras considerables durante esta última década, es así que los ataques en línea han crecido uniformemente, entre estos se encuentra la denegación de servicio (DoS- Denegación de Servicios), en especial cuando es distribuido (DDoS), este ataque realiza una sobrecarga y niega el acceso a una red determinada.

El ataque de esta práctica se realiza con frecuencia en TCP/IP, ya que contiene los protocolos más utilizados para comunicación como es mediante inundaciones de HTTP (Protocolo de Transferencia de Hipertextos) la cual accede a la publicación de datos en internet, generalmente utiliza servicios WEB, las inundaciones abren conexiones TCP con el servidor web, enviando peticiones al servidor, por lo que se sobrecarga el servidor de distintas maneras impidiendo se pueda leer las peticiones simultáneamente (Bezzi, 2016).

La victima tiene pocas posibilidades de detectar este ataque sobre cualquier servidor conectado a internet, cuando el ataque es inyectado, puede afectar diferentes equipos o servicio que se esté utilizando. Se puede prevenir a los usuarios de cómo puede ser la localización de programas malicioso, si observa que una máquina se encuentra comprometida debe dar aviso al administrados de red para que él pueda solucionarlo

el mismo que debe establecer una configuración optima sobre esta y sus respectivas seguridades.

Para realizar un monitoreo de los ataques se ha utilizado la herramienta Wireshark, esta es una herramienta multiplataforma utilizada para detectar paquetes de red, es de gran utilidad por su interfaz amigable al usuario, dentro del análisis se puede detectar conexiones ocultas del propio programa maligno con direcciones remotas para obtener información como inundaciones de denegaciones de servicio. Cuando se captura el tráfico que se está analizando es factible filtrar los paquetes capturados de acuerdo con lo que se está analizando.

Dentro de esta práctica se utiliza la herramienta open-source HOIC (Higth Orbit ION Cannon), diseñada para preservar la red y brindar estabilidad al momento del ataque de inundaciones HTTP ya que contiene una gran velocidad en las tareas de multi-thread, lo que permite bloquear la entrada a las páginas atacadas de esta manera se provoca malestar y pérdida de tiempo al usuario atacado (IMPERVA, 2019).

La herramienta puede ser intimidante al momento de realizar los ataques ya que se puede realizar cambios en los boosts y generar ataques personalizadas, silenciosos, inundaciones por diferentes estados de tiempo lo que impide acceder a la información.

La herramienta HOIC es muy potente al bloquear una página web o reducir la velocidad de procesamiento y por ende la rapidez de respuesta al usuario final. Los problemas legales que conlleva este tipo de ataques pueden ser fuertes, ya que el atacante no permite entregar el control de esta para poder parar el ataque, por lo que no tiene esta configuración en el programa.

Con HOIC, se puede denegaciones de servicio a diferentes páginas ya sea con la URL o IP de esta, el tipo de velocidad del ataque puede variar dependiendo a la configuración inicial, esto ocasiona que la inundación se realice en cuestión de segundos, lo que afecta al usuario de la página atacada. Se realiza el ataque DDoS, mediante las inundaciones de información a través de hilos lo que permite que el servidor se sobrecargue y no pueda procesar toda la información que se inyecta de esta manera el servicio que presta la página deja de funcionar por un lapso.

Para que el programa Anonymous High Orbit Ion Cannon.exe trabaje sin ningún problema se recomienda desactivar el firewall luego de esto se debe realizar el ataque con la herramienta HOIC en un máximo de una hora, ya que el programa Anonymous desaparece de la carpeta en el tiempo antes descrito. Adicional se debe desactivar el proxy si lo tiene en la red porque cuando realiza el ataque este no se ejecuta en la web que desea caso contrario le desconecta de la red interna del proveedor de internet, esto depende de las seguridades de su red.

La herramienta HOIC puede llegar a ser muy peligrosa con personas semi experimentadas ya que es posible modificar opciones de un ataque más personalizado, en donde el impacto en comparación con la configuración estándar es superior. Es una herramienta muy útil, pero si se utiliza de manera inadecuada puede traer problemas legales.

El procedimiento para poder realizar una denegación de servicios utilizando la herramienta HOIC se la realiza en la práctica N° 3 que se detalla a continuación.

3.2.3.1 Título de la práctica

Denegación de Servicios utilizando la herramienta HOIC

3.2.3.1.1 Objetivo general

Analizar un ataque a través de Wireshark mediante herramienta HOIC (Higth Orbit ION Cannon) a una página pública o privada y determinar los tipos de inseguridades que se tiene cuando se ingresa al internet.

3.2.3.1.2 Objetivos específicos

- Determinar las maneras de seguridad que debe tener un usuario cuando realiza navegaciones al internet y de esta forma evitar infiltraciones a su información personal que maneja en su computador.
- Ejecutar inundaciones HTTP a páginas públicas, privadas a través de HOIC, visualizar las pérdidas que ocasionan durante el ataque y la manera de prevenir las agresiones.
- Conocer el tráfico de entrada, salida mediante Wireshark y visualizar la saturación de los puertos con el flujo de información de la página a la que se ejecuta la agresión mediante sobrecargas que impida la actividad por un determinado tiempo.

3.2.3.1.3 Actividades Por Desarrollar

- Se debe realizar esta práctica tomando en consideración los perfiles de permisos de administradores o seguridad de la red que se conecta para realizar el ataque.

- Se debe realizar mediante la URL de la página web o la IP de esta, e identificar el tiempo fuera de servicio, es importante que para realizar esta ejecución se debe desactivar el antivirus que se encuentra instalado en la máquina a realizar la práctica, adicional a esto el tiempo de prueba de HOIC es de una hora.
- Para realizar esta práctica se necesita descargar el archivo .rar (https://mega.nz/#!WdATUALB!bHUy2f44zKLPlsM1doIw_GaJrO7QUUOxXfR3nAhoP7s) y ejecutar los pasos como se detalla.
- Dentro de la herramienta se puede ir modificando la velocidad del ataque que se desea realizar bajo, medio, alto esto depende de las directrices indicadas por el profesor.

3.2.3.1.4 Resultados obtenidos

La denegación de servicio inyectada a la página de escuela comercial de la CNT (www.escuelacomercial.cnt.gob.ec), determina la caída de esta por un lapso de 30 segundos antes que su servidor restaure e identifique el ataque y lo asegure.

Al realizar otro ataque simultaneo identificando que a través de la IP que se realiza el ataque ya no se puede repetir el mismo proceso, esto debido a que el servidor al cual se está haciendo la denegación del servicio identifica el ataque y lo bloquea por seguridades, por esta razón se evidencia que la herramienta HOIC es muy poderosa, hay que considerar que estos ataques que se realiza son a modo de investigación y no para uso de beneficio o afectación a los individuos o compañías públicas o privadas.

En la parte de anexos se encuentra la práctica 3, donde se describe paso a paso cada una de las actividades, incluyendo procedimientos, conclusiones, recomendaciones y bibliografía.

3.2.4 Análisis y recuperación de archivos eliminados de un dispositivo de almacenamiento

3.2.4.1 Disco Duro

El disco duro es el encargado de almacenar toda la información en el computador. El disco es uno de los elementos principal de un computador. El cual contiene varios discos o platos donde cada plato tiene dos cabezas de lectura y escritura. Todas se conectan a un brazo para el acceso y movimiento independiente de lectura y escritura (Dona, 2018).

La distribución de un disco duro se compone de sector de arranque, espacio particionado, impulsor de cabezal, cilindros, clúster y la estructura lógica conlleva volúmenes homogéneos con sistema operativo MS-DOS.

- Sección de arranque (BOOT)
- Tabla de asignación de archivos (FAT)
- Directorio Raíz
- Lista de datos para archivos y subdirectorios

El proceso de lectura inicia cuando los cabezales de lectura o escritura esperan el primer dato que gira con los platos para leer o escribir la información ingresada (Dona, 2018).

3.2.4.2 Memorias Flash

La memoria USB es una actualización de la memoria EEPROM que permite que varias partes de la de memoria sean utilizadas o eliminadas en una misma ejecución de programación por medio de impulsos eléctricos, no como las anteriores que sólo permite grabar o eliminar una celda a la vez EPROM (Dona, 2018).

3.2.4.3 Recuperación de archivos

Los archivos ofimáticos y multimedia se escriben en los dispositivos de acopio en posiciones específicas que se guardan mediante índice, de esta manera el índice indica las partes que se encuentran ocupadas o llenas por información que contenga el usuario de manera automática.

Cuando se borra un dato, lo que se hace es indicar en el índice que ahora la parte donde se encontraba el dato ahora se encuentra libre para luego grabar otros datos sobre esta posición. El dato que se borra sigue en la unidad de almacenamiento solo que el lugar que ocupa en él está como espacio libre para poder sobrescribirlo (CursoHacker, 2014).

Sabiendo todo esto sobre el almacenamiento de archivos en un dispositivo, se considera los siguientes aspectos para poder saber la probabilidad de efectividad de la recuperación de archivos:

- **Datos públicos o privados**: si se está recuperando archivos que se puede volver a descargar, no tiene sentido invertir horas para realizar la recuperación. Si se recupera datos personales, por lo que son únicos, entonces si hay que realizar el análisis del dispositivo de almacenamiento y aplicar la esta actividad de recuperación (CursoHacker, 2014).
- **Cuanto tiempo a transcurrido a partir del borrado de los datos:** el éxito de recuperar un dato reduce cada minuto que el computador está prendido. Esto es porque el dato borrado en la unidad de almacenamiento, pero está en un lugar donde se marca como libre, por lo que pueden sobrescribirse los datos. mientras pasa el tiempo, disminuye la posibilidad de que se recuperen los datos. Tratar de recuperar datos borrados días atrás, si se trabajado con el

equipo todos los días, existe una menor posibilidad de éxito (CursoHacker, 2014).

- **Volumen de archivos guardados después de borrar los archivos que quieres recuperar:** esto tiene que ver mucho con el anterior punto, influye el tiempo y también lo que se ha realizado. Si desde que se borró los datos que se busca se ha grabado varias cosas en el dispositivo de almacenamiento, es probable que se haya sobre grabado los datos borrados, es por esto que la probabilidad de éxito es baja (CursoHacker, 2014).
- **Cuanto ocupan los archivos borrados:** los archivos pesados son los que tienen unos 700 MB aproximadamente o más. Para recuperar un archivo con éxito hay que recuperarlo en su totalidad. Por lo que cuanto mayor espacio ocupa en la unidad de almacenamiento, existe más probabilidad de que se haya perdido una parte de este (CursoHacker, 2014).
- **El tipo de los archivos borrados:** puede ser que se recupere solo una parte si se trata de archivos de imágenes o documentos, pero de todos modos este si es comprensible, para programas no es así, es obligatorio rescatar todo o no funciona.

Luego de analizar todos estos aspectos, se puede determinar la probabilidad de recuperar uno u otro tipo de archivos, en forma general se puede decir que si se trata de recuperar un archivo pesado que fue borrado hace muchos días, es muy probable que no se tenga éxito. En cambio, si se trata de recuperar un archivo pequeño que fue borrado hace muy poco tiempo, de seguro se puede tener éxito en la recuperación de dicho archivo (CursoHacker, 2014).

En esta ocasión utilizamos RecoverIT, herramienta muy potente y avanzada que puede recuperar datos perdidos, anulados o inaccesibles de la unidad de almacenamiento interna o externa. Tiene varios escenarios de recuperación como:

- Archivos borrados
- Papelera de reciclaje
- Disco formateado
- Partición perdida
- Dispositivos externos
- Datos de ataque de virus
- Datos de bloqueo del sistema
- Recuperación integral

Se realiza la identificación y familiarización de la herramienta Recoveryit para el análisis de unidades de almacenamiento utilizando el conjunto de técnicas y procedimientos que posee dicha herramienta que permite la recuperación archivos que fueron eliminados intencionalmente o por equivocación, de una unidad de almacenamiento externo.

Los dispositivos de almacenamiento manejan sectores para almacenar la información y también un sector principal donde se almacena la dirección de cada archivo almacenado, cuando se elimina o se formatea lo que se elimina es este sector principal y cuando se graba información adicional, esta se sobrescribe en el sector donde se encontraba la información eliminada, es por eso que la información se puede recuperar tomando en cuenta que no se ha realizado un almacenamiento adicional después de eliminar la información.

El Disco Duro es uno de los componentes importantes del computador, ya que es ahí donde se instala lo primordial para el perfecto funcionamiento del equipo que utilizamos y también es donde almacenamos todos los datos. Es por eso qué al momento de realizar el análisis de los sectores hay que tener mucho cuidado para el éxito de la recuperación.

RecoverIT es una herramienta de recuperación de información que se haya borrado, pero si se recupera información que se encuentra en el disco donde se encuentra instalado el sistema operativo no es recomendable instalar el aplicativo ya que al realizar esto se estará sobrescribiendo sectores que posiblemente fueron ocupados por información que se quiere recuperar.

Cuando falla una PC de escritorio, y para recuperar los datos sólo se tiene una notebook, no tendremos como conectarlo, es decir no tendremos un puerto adecuado para leer el disco del equipo con fallas a la portátil. Por lo que es recomendable adquirir un dispositivo que permita hacer esto con comodidad, estos son los disks case, los cuales son un convertidor de datos a USB en el cual tendremos que conectar el disco duro para posteriormente poder leer el disco mediante el puerto USB.

El procedimiento para poder realizar el análisis y recuperación de archivos eliminados de un dispositivo de almacenamiento se la realiza en la práctica N° 4 que se detalla a continuación.

3.2.4.4 Título de la práctica

Análisis y recuperación de archivos eliminados de un dispositivo de almacenamiento con la herramienta RECOVERYIT.

3.2.4.4.1 Objetivo general

Realizar la identificación y familiarización de la herramienta Recoveryit para el análisis de dispositivos de almacenamiento, utilizando un conjunto de técnicas y procedimientos que posee dicha herramienta que permite la recuperación de archivos que fueron eliminados intencionalmente o por equivocación, de un dispositivo de almacenamiento externo.

3.2.4.4.2 Objetivos específicos

- Habituarse con la herramienta Recoveryit en el recobro de los datos borrados dentro de una unidad externa.
- Asemejar los registros anulados de la unidad de acopio externa que es examinado con la herramienta Recoveryit.
- Rescatar los registros eliminados que estuvieron identificados dentro de la unidad externa.

3.2.4.4.3 Actividades por desarrollar

Para desarrollar esta actividad de estudio de discos externos o internos, se debe primero eliminar la información que estos contengan o inclusive ejecutar un formateo para luego proceder al recobro de la información eliminada.

El software que se ocupa es Recoveryit que se encuentra licenciado y se descargar desde la página oficial del fabricante, adicional a la descarga se necesita el crack para conseguir las funcionalidades de la herramienta.

3.2.4.4.4 Resultados obtenidos

Terminada la práctica en la que se ejecuta el borrado de la información de una unidad externa o ejecutando un formateo del dispositivo se establece el estudio con la herramienta, ya que admite representar los registros que se excluyeron en el dispositivo de acopio mediante índices a elegir en la recuperación de información. Con esto el estudiante está en la capacidad de recuperar información eliminada de un dispositivo externo.

En la parte de anexos se encuentra la práctica 4, donde se describe paso a paso cada una de las actividades, incluyendo procedimientos, conclusiones, recomendaciones y bibliografía.

3.2.5 Creación de imagen a partir de una unidad de almacenamiento

FTK Imager es una herramienta que advierte el uso directo o indirecto de la evidencia digital, realiza duplicidad de bit a bit de la imagen hacer estudiada añadiendo los espacios libres o vacíos del dispositivo manteniendo la veracidad de la información original, se realiza con toda la parte del disco o particiones que posteriormente pueden ser reformadas. El software admite realizar búsquedas de directorios, archivos extraviados mediante palabras claves.

Al finalizar la captura de la imagen, el software genera un clave hash MD5 que es utilizada para confirmar la integridad de los datos versus la unidad de almacenamiento original y verificar que la imagen que hemos creado no ha sido alterada, esto tomando en cuenta que cualquier tipo de cambio por más mínimo que haya sido en el archivo de imagen, esto se ve reflejado en la integridad de la imagen realizada (Suárez & Martínez, 2016).

Se debe ejecutar la creación de imagen de un disco para el análisis del contenido, aplicando hashing o la revisión de la probidad del perfil del disco, así como el asedio de escritura de la imagen, para investigar y confirmar los archivos de la imagen hecha sin perturbar la integridad de la unidad origen.

FTK es una herramienta que obtiene imágenes de discos duros locales, unidades de memoria USB, carpetas, archivos individuales u otros, para realizar un análisis forense completo y obtener un informe con todos los hallazgos localizados en el perfil y de esta manera preservar la evidencia original sin alteraciones sobre la prueba fehaciente.

Con la imagen derivada de FTK se tiene una perspectiva amplia sobre el contenido de los datos en relación con el hash que se utiliza para comprobar la veracidad de la información, los cuales deben ser exactos antes y después de la clonación de la imagen y con ello impedir manipulaciones sobre las pruebas recolectadas ante una investigación.

FTK necesita una gran capacidad de almacenamiento ya que crea varios archivos con un tamaño de 1.5 GB de una copia de imagen de 32 GB lo cual proporciona velocidad de procesamiento, estabilidad y facilidad de uso, que es muy intuitiva para el usuario.

Es importante cuando se ejecute la copia de imagen mediante FTK se realice un bloqueo de escritura para evitar cambios en el disco y de esta manera mantener seguridad y confiabilidad en los datos hacer analizados por el investigador.

El procedimiento para poder realizar la creación de imagen a partir de una unidad de almacenamiento se la realiza en la práctica N° 5 que se detalla a continuación.

3.2.5.1 Título de la práctica

Creación de una Imagen para el análisis digital forense mediante la herramienta FTK Imager en el Sistema Operativo Windows.

3.2.5.1.1 Objetivo general

Instituir una clonación de disco para analizar la información que almacena mediante la ejecución de hashing o la comprobación de la probidad de la clonación del disco y el cerco de escritura de la imagen sin perturbar la integridad del dispositivo de arranque.

3.2.5.1.2 Objetivos específicos

- Entender el funcionamiento del programa FTK Imager que permite extraer una imagen de una unidad de almacenamiento interno o externo para su posterior análisis sin dañar la integridad origen.
- Entender lo que representan el hashing MD5 y SHA1 en las unidades de almacenamiento y las imágenes, para verificar su autenticidad con la unidad origen.
- Adquirir registros de Imagen de los elementos de acopio que es la esencia de evidencia digital ante un delito, para ser examinado sin estropear la integridad de los datos crudos.

3.2.5.1.3 Actividades por desarrollar

Se requiere descargar el software de FTK IMAGER 3.4.3 para la clonación de imagen y el estudio de unidades de acopio interno o externo.

3.2.5.1.4 Resultados obtenidos

Una vez terminada la práctica el principal resultado son los archivos de Imagen que permiten realizar análisis sin afectar la integridad de la unidad de almacenamiento original.

También se tiene el archivo que admite visualizar toda la información de seguridad y especificaciones de la unidad de almacenamiento origen.

Se muestra el detalle de cada archivo y carpeta que contiene la unidad de almacenamiento de la cual se realizó la imagen.

En la parte de anexos se encuentra la práctica 5, donde se describe paso a paso cada una de las actividades, incluyendo procedimientos, conclusiones, recomendaciones y bibliografía.

3.2.6 Estudio Forense de Archivos Multimedia en WHATSAPP

Los equipos móviles son necesarios en el trabajo, hogar, estudio, investigación, comunicación, relaciones sociales entre otros aspectos ya que permiten mantener una comunicación bidireccional en tiempo real.

3.2.6.1 Usuario de Root en equipo móvil

Root significa raíz, equivale adquirir los permisos completos en el dispositivo para realizar modificaciones o eliminaciones al sistema operativo, desde este punto de vista este súper usuario permite manipular la información generada en aplicaciones como mensajes, contactos, llamadas, archivos multimedia, etc. En ocasiones no es indispensable que el equipo tenga la inmunidad de ser root para extraer la información de modo transitorio o constante, es importante identificar el tipo de proceso que se ejecuta de acuerdo con el sistema operativo, fabricante, modelo y versión de los equipos a ser estudiados.

3.2.6.2 Seguridad del Sistema Android

El sistema operativo Android al igual que otros tipos de sistemas posee sus propias seguridades, certificados, firmas que permite identificar el dueño de la creación, así como la versión, fecha de creación, dirección, modelo entre otros aspectos que caracterizan al administrador del S.O.

3.2.6.3 Depuración USB

Está diseñado para desarrolladores, ya que permite el acceso al sistema SDK (Software Development kit) Android, que es requisito para la conexión entre cable de transferencia de datos en el móvil y el computador y se pueda realizar la copia bit a bit (INCIBE-CERT, 2019).

3.2.6.4 Kali Linux

Kali está basada en Debian y mantenido por Offensive Security, su objetivo es realizar la penetración de la seguridad a paquetes que sean convenientes para el ejecutador, además ofrece herramientas de código abierto para ejecutar pruebas de seguridad y posteriormente ser analizadas. Kali posee un entorno gráfico amigable al usuario, puede realizar amenazas reales sin fines educativos y generar problemas, es una herramienta basada en seguridades (MXL, 2019).

3.2.6.5 Adb

Android Debug Bridge (Adb), es una línea de comando que se ejecuta en Kali Linux para relacionar de manera física o virtual un dispositivo que tenga sistema operativo Android con el computador.

3.2.6.6 Fastboot

Es un protocolo móvil que permite realizar modificaciones en los sistemas de ficheros mediante una conexión USB a un dispositivo Android (INCIBE-CERT, 2019).

3.2.6.7 Guasap Forensic

Es una aplicación que permite realizar peritajes informáticos de base de datos de conversaciones, logs, archivos multimedia de WhatsApp, sin alterar el archivo original, basado en Python bajo la licencia Pública General GNU. La aplicación realiza un proceso de extracción de información probatoria ya que se refleja el contenido de mensajes transmitidos en las redes sociales como en este caso se utiliza WhatsApp. La herramienta que se utiliza tiene una licencia GNU, lo que permite obtener los archivos multimedia pero no se puede imprimir un informe que esa opción si se la tiene en una licencia pagada GNU3 (INCIBE-CERT, 2019).

Se realiza un análisis de archivos multimedia que se extraen a través de la herramienta Guasap Forensic en un dispositivo móvil de marca LENOVO con sistema operativo Android mediante máquina virtual Kali-Linux, sin alterar la información origen del equipo y de esta manera preservar la evidencia del usuario.

Kali es diseñado para realizar auditoría sobre seguridad informática mediante ejecución de comandos como Guasap Forensic, esta aplicación realiza valoraciones informáticas al sistema operativo Android, extrayendo los contenidos de la base de datos de WhatsApp, como conversaciones, logs, archivos multimedia, sin perturbar la base única analizada.

Guasap Forensic es utilizada en averiguaciones forenses computaciones ya que realiza un proceso de reproducción de bit a bit al computador del investigador con su

hash, esto instituye una comunicación de los medios de mensajería instantánea, precautelando los datos crudos.

La versión profesional permite tener un análisis profundo, técnico y jurídico que deriva a autenticar archivos multimedia, Logs, mediante conversaciones mantenidas en WhatsApp, la versión que se utiliza en este estudio es a modo de prueba lo que implica no obtener todos los datos al 100% para el estudio que se realiza.

La investigación mediante Guasap Forensic, en un dispositivo móvil Android, debe estar actualizado, rooteado y activado el modo de depuración de USB, para que la aplicación pueda extraer los datos que se aloja en la base de WhatsApp, el contenido lo extirpa de conversaciones activas, inactivas o mensajes borrados, cabe recalcar que si la herramienta se encuentra licenciada mediante un medio de pago emite un informe completo del análisis realizado.

El procedimiento para poder realizar un Análisis Forense de Archivos Multimedia a través de WHATSAPP se la realiza en la práctica N° 6 la cual se describe a continuación.

3.2.6.8 Título de la práctica

Análisis Forense de Archivos Multimedia a través de WhatsApp, para sistema operativo Android utilizando herramienta GUASAP FORENSIC ejecutada en KALI LINUX.

3.2.6.8.1 Objetivo general

Realizar un análisis de archivos multimedia eliminados que se extraen a través de la herramienta Guasap Forensic en un dispositivo móvil de marca LENOVO con

sistema operativo Android mediante máquina virtual Kali-Linux, sin alterar la información origen del equipo y de esta manera preservar la evidencia del usuario.

3.2.6.8.2 Objetivos específicos

Conseguir contenido multimedia borrado como imágenes, audios, videos, gif que intervinieron en una conversación simple o compuesta de WhatsApp, precautelando la veracidad del contenido.

Estudiar el contenido multimedia y registros borrados en el aparato móvil de marca LENOVO versión 5.1.

Identificar las ramificaciones de cada uno de los registros multimedia, como las fechas, tamaño, alteraciones elaboradas interiormente en el celular móvil.

3.2.6.8.3 Actividades por desarrollar

Tomar en consideración los perfiles de administración de la red para la ejecución del estudio de archivos multimedia con la herramienta Guasap Forensic.

Instalar una máquina virtual KALI –LINUX con un espacio de 30 GB, para instalar los ejecutadores de base de datos y rooteadores que se necesita para que funcione la herramienta Guasap Forensic.

En el dispositivo móvil con el que se realiza pruebas debe estar configurado a modo de root, adicional a esto debe tener activa la depuración de USB que permite realizar la extracción de la información sobre los archivos multimedia compartidos mediante conversaciones bidireccionales en WhatsApp.

3.2.6.8.4 Resultados obtenidos

Durante la ejecución de la práctica se obtiene resultados favorables para el análisis de archivos multimedia como las siguientes extensiones que se detalla a continuación: (Jpg, Mp4, Docx, Pdf, xls). Al separar los registros se identifica el nombre, fecha de modificación, tipo, tamaño lo que interesa como prueba durante un juicio siempre y cuando no coexistan variaciones sobre los mismos.

Las deducciones periciales sobre documentos y registros aportan a igualar el principio de la comunicación, la originalidad de sus autores, probidad y seguridad de los datos investigados.

En la parte de anexos se encuentra la práctica 6, donde se describe paso a paso cada una de las actividades, incluyendo procedimientos, conclusiones, recomendaciones y bibliografía.

3.2.7 Estudio de imagen de una unidad de acopio externo con la herramienta Autopsy

Autopsy es un software que abarca todas las utilidades que brida “The Sleuth Kit”, presenta un esquema gráfico que modela los efectos del estudio forense de clonaciones de imágenes, Esto proporciona a los investigadores evidencia en un efímero tiempo y de manera organizada. Las características principales de la herramienta son (Suárez & Martínez, 2016).

- Es extensible: el interesado puede añadir hechos funcionalidades, complementos que logren examinar el origen de fichas que se está estudiando (Suárez & Martínez, 2016).

- Es fácil de usar: el buscador de Autopsy ofrece los asistentes y las herramientas históricas para que los usuarios puedan repetir sus pasos sin demasiada reconfiguración (Suárez & Martínez, 2016).

Es una herramienta que sirve para organizar y analizar todas las evidencias que son objetos de investigación. Tomando en cuenta la gran cantidad de opciones que se requiere para dicho análisis (Suárez & Martínez, 2016). A continuación, se describe algunas de las funciones básicas que posee esta herramienta son:

- **Análisis de archivos:** muestra la imagen como archivo y directorios permitiendo ver incluso aquellos que son ocultos por el sistema operativo (Suárez & Martínez, 2016).
- **Búsqueda por palabra Clave**: permite buscar dentro de la imagen palabras clave que pueden ser archivos o cualquier otra referencia que sea tomada como argumento en el informe pericial (Suárez & Martínez, 2016).
- **Tipo de archivo:** permite la búsqueda y ordenación de archivos según su tipo y/o extensión (Suárez & Martínez, 2016).
- **Detalle de la Imagen**: muestra el detalle de la imagen a examinar, lo cual permite saber dónde se encuentra físicamente la información de dicha imagen (Suárez & Martínez, 2016).
- **Metadatos:** visualiza los elementos del sistema de archivos que normalmente no se muestran, como son las referencias o directorios de archivos eliminados (Suárez & Martínez, 2016).
- **Unidad de Disco:** tiene la posibilidad de entender con mayor detalle cualquier tipo de archivo, y de esta manera examinar más a fondo el archivo, ya sea en su código ASCII o Hexadecimal (Suárez & Martínez, 2016).

Se realiza el análisis completo de la imagen que se ha montado al momento de obtener la evidencia digital, con la herramienta Autopsy compatible con sistemas operativos Windows.

Con la herramienta Autopsy se puede extraer información de dispositivos externos de memoria y de esta manera lograr un análisis estructurado preservando los datos originales sin realizar alteraciones en los archivos crudos, lo que permite tener una evidencia legitima ante un proceso de investigación pericial informática forense.

Autopsy logra realizar un análisis por tipo de archivos, tiempo de actividad de los archivos, búsqueda por palabra clave, metadatos, unidades de datos, manejo de casos, registro de sucesos, eventos entre otros, todo lo antes detallado permite al investigador forense adquirir un conocimiento real sobre los hechos analizados y de esta manera emitir un informe pegado a la realidad de un ataque o infiltración de seguridad.

Al momento de realizar un análisis de la imagen del dispositivo con Autopsy es importante verificar que no exista ningún tipo de alteraciones ya que esto puede comprometer el cálculo de MD5 y HASH, esto con la finalidad que el estudio sea íntegro y verídico.

Cuando se realiza el estudio de una imagen a través de Autopsy es recomendable verificar que el computador tenga suficiente capacidad de almacenamiento esto dependerá de la imagen la cual se realizará el análisis.

La manera para efectuar el estudio de imágenes mediante Autopsy se la cumple en la práctica N° 7 la cual se relata a continuación.

3.2.7.1 Título de la práctica

Análisis de imagen de un dispositivo de almacenamiento externo mediante la herramienta Autopsy.

3.2.7.1.1 Objetivo general

Realizar el análisis completo de la imagen que se ejecuta al momento de obtener la evidencia digital, con la herramienta Autopsy compatible con sistemas operativos Windows.

3.2.7.1.2 Objetivos específicos

- Interactuar con la herramienta Autopsy y toda la gama de parámetros que se puede examinar en un caso de informática forense.
- Realizar un análisis forense digital siguiendo una estructura metodológica que permite clasificar la evidencia recolectada.
- Comprobar la probidad de la efigie entregada para el estudio.
- Tener una documentación estructurada de la evidencia recogida.
- Seleccionar la información que sirva como evidencia probatoria en una acción delictiva.
- Emitir un informe completo del análisis realizado.

3.2.7.1.3 Actividades por desarrollar

- Para perpetrar el examen del contenido es ineludible tener la imagen en formato. ddd, la cual se indica en las prácticas sobe creación de imagen.
- El software que se utiliza es Autopsy, es un software libre que se puede descargar de la página oficial https://www.autopsy.com/download/.

3.2.7.1.4 Resultados obtenidos

Se evidencia el estudio de un flash memory de 32 GB, Autopsy admite cumplir un informe completo de la investigación que consigue ser cuerpo de evidencia al instante de dictar sentencia en el delito que se esté inquiriendo.

En la parte de anexos se encuentra la práctica 7, donde se describe paso a paso cada una de las actividades, incluyendo procedimientos, conclusiones, recomendaciones y bibliografía.

3.2.8 Análisis de Información de una PC con sistema operativo Windows mediante herramienta OSForencis

La investigación que se realiza dentro de la herramienta OSForensics, requiere de información que contenga evidencia electrónica que pueda aportar para un análisis digital forense y de esta manera se pueda contener los datos sin ser alterados, entre estos tenemos: fecha de inicio a las carpetas que se encuentran alojadas en la computadora o aplicaciones web, Registro de accesos a ficheros, Almacenamiento de cookies en el disco duro Procesos de ejecuciones de la computadora, Archivos eliminados, Escaneo de usuarios y contraseñas (PassMark, 2019).

OSForensics es una herramienta desarrollado por Passmark, que se utiliza en investigación forense digital, ya que permite encontrar información visible, oculta o eliminada dentro del análisis de un computador, la herramienta es muy amigable al usuario y permite llevar un orden de extracción de datos de acuerdo con la necesidad del investigador (PassMark, 2019). OSForensics trabaja en 3 fases:

1. Descubrimiento
2. Identificación
3. Administración

Se efectúa un análisis de investigación sobre la información que se extrae de un sistema operativo Windows, mediante herramienta OSForencis y se identificó los tipos de actividades que se realizó en la computadora.

Mediante la herramienta OSForensics se extrae información como la exploración de actividades recientes, exploración de contraseñas en sitios web, análisis de disco, análisis de equipos conectados mediante USB, documentos recientes de Windows, historial de navegación, descargas realizas entre otros procesos los que permite adjuntar pruebas fehacientes durante la investigación.

El contenido que se extirpa con OSForensics, consigue acumular en un disco extraíble para en lo posterior se pueda estudiar de manera cautelosa sin afectar la probidad y seguridad del contenido crudo.

La herramienta OSForensics tiene un tiempo de prueba de 30 días para realizar el análisis del equipo con sistema operativo Windows, cabe indicar que algunos procesos no se pueden exportar en sus extensiones originales como por ejemplo documentos de office, lo cual no permite tener una información legible para la investigación, la versión pagada tiene todos los privilegios en los procesos que contiene la herramienta ya que está destinada para administradores, investigadores de ciberseguridad de pequeñas y grandes empresas.

Para la disposición de OSForensics es obligatorio poseer un área de disco de 60GB y una memoria RAM de 1GB, para formar todos los anejos que sobrelleva la aplicación, además es significativo aludir que el contenido que se desentierra se debe manipular con comportamiento profesional.

El procedimiento para poder realizar un Análisis de Información de una PC con sistema operativo Windows mediante herramienta OSForencis se la realiza en la práctica N° 8 la cual describe a continuación.

3.2.8.1 Título de la práctica

Análisis de Información de una PC con sistema operativo Windows mediante herramienta OSForencis.

3.2.8.1.1 Objetivo general

Efectuar un análisis de investigación sobre la información que se extrae de un sistema operativo Windows, mediante herramienta OSForencis e identificar los tipos de actividades que se realiza en la computadora.

3.2.8.1.2 Objetivos específicos

- Obtener información visible, oculta o eliminada para adquirir evidencia necesaria para un análisis profundo y completo en un reporte que sea presentado ante un proceso judicial.
- Identificar los diferentes archivos y sus respectivas extensiones, manejar de manera prudente los datos obtenidos sin perjuicio al victimario.

3.2.8.1.3 Actividades por desarrollar

- Efectuar un estudio de cada uno de los registros que cuenta la herramienta OSForensics y lograr un examen de los acontecimientos que se cumple en la máquina a ligar.
- Se debe verificar la capacidad de disco duro y memoria RAM del equipo que se analiza, para que se pueda instalar el programa OSForensics sin problemas.
- Verificar y analizar los reportes entregados por la herramienta e identificar las evidencias válidas que puedan ingresar ante un proceso judicial a ser investigado.
- Algunos de los registros que contiene OSForencis, no se hallan habilitadas por la versión a prueba, se debe tener en cuenta al instante de cumplir la observación de los datos conseguidos.

3.2.8.4 Resultados obtenidos

Con la extracción del contenido al equipo mediante OSForensics, se adquiere efectos limpios y seguros, que se analizan de acuerdo al tiempo de ejecución, dirección de ficheros, cookies grabados en el disco, usuarios y contraseñas de acceso aplicaciones web, ente otros que logran conseguir datos concluyentes y únicos sin trastornar el contenido crudo del computador. Los resultados obtenidos son:

- Lista de procesos Volcado de memoria física
- Exploración de actividad reciente
- Exploración de contraseña
- Exploración de archivos eliminados
- Generar nuevo informe HTML
- Usuarios y Contraseñas de red WIFI
- Búsqueda de archivos

Al abrir cada uno de estos archivos se puede identificar el tamaño, fecha o modificación de cada uno de estos, esto sirve como prueba durante un juicio siempre y cuando no existan alteraciones sobre los mismos.

Estos resultados periciales sobre documentos y archivos aportan a identificar el origen de la comunicación y sobre todo la integridad y seguridad de la información analizada.

En la parte de anexos se encuentra la práctica 8, donde se describe paso a paso cada una de las actividades, incluyendo procedimientos, conclusiones, recomendaciones y bibliografía.

3.2.9 Estudio de Memoria RAM con Volatility Framework en KALI-LINUX

Kali Linux posee algunas formas que acceden a poner en experimento la seguridad y confiabilidad de una estructura operativa y de este modo asemejar posibles agresiones informáticas.

La herramienta Volatility Framework puede encontrar archivos DLL ocultos en la memoria RAM de acuerdo con las etiquetas que poseen, lo que permite identificar algún código inyectado que ocasione problemas en la ejecución de los procesos. Para extraer la información de la memoria RAM de Windows XP en Kali se utiliza la siguiente línea de comandos los cuales permite ver obtener datos reales sobre el equipo que se está analizando (Volatilidad, 2018). Entre estos comandos se tiene:

Pslist: permite listar los procesos que se encuentren activos en ese instante.

Connections: permite listar las conexiones que se encuentran abiertas.

Sockets: permite listar sockets que se encuentran abiertos.

Connscan: explora la memoria física en busca de objetos de conexiones TCP.

Dlliist: imprime la lista de archivos DLL que se cargan en cada proceso.

Getsids: extrae los SID’s que tiene cada proceso.

Hivescan: explora la memoria física en busca de secciones de registro.

Una vez que se realiza el análisis de los procesos del dump de la memoria RAM cridex.vmem, se identifica procesos extraños que se ejecutan en la misma hora lo que es posible que estos procesos se encuentren infectados de malware (Volatilidad, 2018).

Para descartar que un proceso se encuentre infectado se extrae el ejecutable del PID sospechoso, de esta manera se analiza mediante herramienta web de virus total, el cual identifica los tipos de malware que se encuentran inyectados dentro del proceso analizado, de esta manera arroja información coherente al investigador. Dentro de esos procesos es de gran importancia la información que se refleja sobre las ip´s de origen ya que con la ayuda de otras herramientas se puede identificar la geolocalización del posible atacante, cabe indicar que la ip puede ser atípica.

Con el análisis de la memoria RAM mediante Volatility Framework y los comandos de búsqueda que se ejecutan en el perfil se puede identificar procesos maliciosos como malware que afectan el funcionamiento del sistema operativo.

Con los PID que se obtienen en la herramienta Volatility Framework de las acciones ejecutables y las ip´s origen del sistema se puede realizar una geolocalización del posible atacante, es importante la información que se extrae para el estudio del investigador forense, cabe recalcar que las ubicaciones pueden ser atípicas, por lo que el estudio conlleva a reunir todas las pruebas recolectadas para dar un informe final.

Cuando se utiliza la herramienta Volatility Framework en Kali Linux, es indispensable tener un conocimiento básico en los comandos como: Pslist, Connections, Sockets, Connscan, Dlliist, Getsids, Hivescan, entre otros ya que con la utilización de dichos códigos se puede realizar la extracción de información de la memoria RAM a ser analizada y de esta manera analizar los datos para formular un informe veraz y seguro.

Al realizar la descarga de la memoria RAM Cridex.Vmem, en la máquina virtual es importante desactivar el antivirus del equipo para evitar que exista problemas en la

ejecución del proceso, además se debe copiar en el directorio de Volatility para realizar las consultas correspondientes a la investigación y evitar inconvenientes cuando se ejecutan los comandos de consultas.

El procedimiento para poder realizar un Análisis de Memoria RAM mediante Volatility Framework en KALI-LINUX se la realiza en la práctica N° 9 la cual describe a continuación.

3.2.9.1 Título de la práctica

Análisis de Memoria RAM mediante Volatility Framework en KALI-LINUX.

3.2.9.1.1 Objetivo general

Realizar un análisis de investigación forense de Memoria RAM, mediante la herramienta Volatility Framework de KALI – LINUX y aplicar comandos de extracción de procesos para el estudio de los datos obtenidos e identificar procesos maliciosos que ocurren dentro de la memoria.

3.2.9.1.2 Objetivos específicos

- Utilizar comandos de la herramienta Volatility Framework que tiene instalada KALI-LINUX y realizar un análisis de la información del Dump de la memoria RAM Cridex.Vmem.
- Analizar los resultados de los comandos ejecutados a través de Volatility Framework e identificar si existe vulnerabilidades en la memoria RAM, así como filtraciones de seguridad en la red.

3.2.9.1.3 Actividades por desarrollar

Para realizar el análisis de Memoria RAM mediante Volatility Framework en KALI-LINUX es importante tener instalada una máquina virtual con el sistema operativo Kali Linux y descargar la memoria Ram Cridex.Vmem, que permite realizar los diferentes estudios de comandos que se ejecuta a través de Volatility, de esta manera identificar los posibles malware que se ejecuta en el equipo, así como también determinar la geolocalización de un atacante con las Ip`s origen que arroje la información solicitada a través de los comandos de consulta.

3.2.9.1.4 Resultados obtenidos

Con los efectos logrados de las instrucciones de Volatility, se obtiene el siguiente estudio:

- Se verifica una discrepancia entre el proceso wuauclt.exe, el cual tiene diferente PID, donde el PID 1136 atrasa del PID 1588 lo que se observa cuando se ejecuta el comando line.
- Existe el usuario S-1-5-21-789336058-261478967-1417001333-1003 (Robert), que ha iniciado procesos en explorer y reader_sl.exe sin ser administrador.
- Se identifica que el proceso reader_sl.exe, se encuentra infectado de malware a través de virus total, el mismo que se extrae de la memoria RAM y se coloca en el disco duro de kali Linux.
- Las ip’s de origen con el cual se inicia el sistema se encuentra en África y la India, pero aun así las ip´s pueden ser atípicas ante una agresión informática.

En la parte de anexos se encuentra la práctica 9, donde se describe paso a paso cada una de las actividades, incluyendo procedimientos, conclusiones, recomendaciones y bibliografía.

3.2.10 Análisis de eventos de sistemas operativo mediante la Herramienta Event Log Explorer

Un log es un registro de actividad de un sistema, que generalmente se guarda en un fichero de texto, al que se le van añadiendo líneas a medida que se realizan acciones sobre el sistema (Paus, 2016). Los formatos de registro de eventos son:

- **Windows:** EVT / EVTX
- **Linux:** .log
- **Bases de datos:** trc
- **Cisco**: .log

Existen diferentes clases de logs que se detallan a continuación:

- Sistema (Registro de evento, Registro de auditoria de usuarios)
- Logs de aplicaciones (Consultas a servidores, Información de uso del aplicativo, Acciones realizadas e Información de cuentas de usuarios registrados)
- Logs de seguridad (Eventos de antivirus, Hips/Hids, Proxy, Routers y Firewall)

Los eventos más importantes de Windows al momento de realizar un análisis forense son se los puede ver en la Tabla 19.

Tabla 19. Eventos más importantes.

Event ID	Descripción
4624	Acceso exitoso
4625	Error de sesión
4672	Administración de cuentas de sesión
4647	Cierre de sesión exitoso
4634	Cierre de sesión exitoso
4771	Error en la pre- autenticación a través de dominio
4768	Controlador de dominio emitió TGT(Ticket Granting Ticket)
4776	Inicio de sesión fallido o exitoso a través de dominio
7034	Servicio caído de forma inesperada
7035	El Servicio envía una señal de arranque o apagado
7036	Detenimiento o Inicio de Servicio
7040	El Tipo de inicio del servicio ha cambiado
5140	Asignación de recurso compartido en la red
4778	Iniciación de sesión RDP
4779	Finalización de la sesión RDP
106	Tarea programada
200	Tarea ejecutada
201	Tarea terminada
141	Tarea Eliminada

Nota: Información Obtenida en: (Paus, 2016)

Para los registros de aplicaciones uno de los eventos que puede ser de gran ayuda al momento de una investigación forense es el evento con el ID: 300, es un suceso avizor de un correo que está por ser borrado (Paus, 2016).

La búsqueda de sucesos de Windows provee un contenido veraz y logra recopilar la evidencia significativa cubierta a los procedimientos sucedidos en el medio (Paus, 2016).

Los principales beneficios de los eventos que son recogidos y almacenados por el Servicio de Registro de Eventos son: Identificar el Evento, Categorías del Evento, Descripción; Marca de tiempo; Identificar los usuarios y sistemas involucrados; identificar a que recursos se accedieron. (Paus, 2016).

Una parte esencial de la investigación de un delito en donde está involucrado un computador es la revisión y análisis del registro de actividades el cual puede ser parte de un elemento comprobatorio en la investigación. El uso de este material admite mejorar el lapso de resultados del investigador, ya que consiente cumplir una sucesión de tamices en los sucesos, así como hallar los elementos comprobatorios de la investigación.

El contenido que posee este tipo de registros proviene de eventos y canjes que normalmente comete en el propio sistema, se requiere de una herramienta externa para mejorar la indagación de los elementos que alcanzan a dominar datos importantes en la exploración del caso.

Es preferible utilizar Logs en los cuales se tiene registrado varios y diferentes actividades Para el análisis y mejor entendimiento de estos, donde se registra todos los eventos del sistema operativo. Para obtener la evidencia encontrada luego de realizar el análisis es necesario generar el reporte que permite entender de mejor manera la información de los registros de eventos del sistema operativo.

Si se encuentra modificaciones en la fecha de creación es indispensable perpetrar un estudio perfecto de las permutas y actualizaciones de los registros de todo el disco investigado desde la fecha que se ejecutó el canje, de modo que se puede exponer un informe justificado en la investigación que se está realizando.

El modo para poder plasmar un Estudio de sucesos de sistemas operativos mediante la herramienta Event Log Explorer se la realiza en la práctica N° 10 la cual se refiere posteriormente.

3.2.10.1 Título de la práctica

Análisis de eventos de sistemas operativo mediante la Herramienta Event Log Explorer.

3.2.10.1.1 Objetivo general

Analizar los Logs del sistema operativo Windows para evidenciar los cambios de configuración importantes en el sistema, como cambio de la fecha y hora utilizando la Herramienta Event Log Explorer.

3.2.10.1.2 Objetivos específicos

- Entender la importación de los archivos de registros de eventos (LOGS) y su interpretación y buen uso al momento de realizar el análisis forense.
- Sacar el máximo provecho de la herramienta Event Log Explorer que permite visualizar el rastro que dejo el usuario en una Computadora.
- Analizar un archivo de registro de eventos para identificar los cambios que se realiza en el sistema operativo.

3.2.10.1.3 Actividades por desarrollar

- Lo primero que hay realizar es obtener la evidencia a ser analizada ya sea mediante una imagen de disco o directamente del sistema operativo.
- Para realizar el análisis de los eventos se debe identificar el delito que se desea estudiar y de esta manera se pueda efectuar la observación y búsqueda de un suceso en específico.
- El software que se esgrime es Event Log Explorer modalidad pago, se realiza la descarga de la cuenta representativa. https://eventlogxp.com/.

3.2.10.1.4 Resultados obtenidos

El estudio de los registros de acciones (Logs) indican sucesos de cambio en el log de seguridad del Sistema Operativo, consecutivamente se adquiere una síntesis de modificación de fecha, la cual representa porción de la realidad en la modificación o transformación de archivos con fechas que no incumben al original.

En la parte de anexos se encuentra la práctica 10, donde se describe paso a paso cada una de las actividades, incluyendo procedimientos, conclusiones, recomendaciones y bibliografía.

3.3 Herramientas de software para implementar en el Laboratorio de Informática Forense

Dentro de las prácticas realizadas en este proyecto se ha identificado una infinidad de ataques informáticos que afectan a personas o instituciones públicas o privadas, esta actividad ha alcanzado niveles avanzados a modo de extraer información para poder extorsionar o denigrar a las personas, lo cual aspira al atacante obtener un beneficio económico, personal o psicológico, esto depende del objetivo que se quiere alcanzar.

Debido al número de ataques informáticos que sufre la población basado en el crecimiento tecnológico y al uso de herramientas que facilitan el desarrollo de delitos ocasionando procesos ilícitos. Es importante describir con un lugar que permita efectuar estudios de datos recogidos como realidad digital, con la intención de asemejar a los posibles prosistas de los ataques, resguardando la probidad, seguridad y reserva del contenido apegado a las normativas que gobiernan dentro del país y de esta cualidad poseer pruebas que alcancen a ser llevadas ante un juicio legal, con el propósito de que los comprometidos sean juzgados y castigados bajos las leyes del Ecuador.

En base a las diferentes prácticas que se plantearon para la implementación del Laboratorio de Informática Forense se puede observar que la gran mayoría de herramientas que se utilizaron son de uso libre por un lapso de prueba, las cuales implicaría un costo al momento de que se decida implementar el Laboratorio de Informática Forense.

Tabla 20. Software utilizado

NOMBRE	CARACTERISTICA	PRECIO
Web Grabify Ip Logger	Proporciona datos estadísticos de sus enlaces y realiza una geolocalización de las direcciones IP	Open source
FotoForensics	Permite verificar la falsedad de una imagen.	Versión gratuita
		Versión completa pagada, valor por un año de $380
H.O.I.C	Aplicación de código abierto que se utiliza para ataques de denegación de servicio DoS.	Open source
Wondershare Data Recovery (Recoverit)	Realiza un escaneo rápido de los procesos analizados, los recupera y restaura.	Versión gratuita es limitada solo a modo de visualización.
		Versión pago por el precio de $69.95
Access Data FTK Imager	Realiza una copia exacta de discos externos como internos	Versión gratuita limitada.
		Versión pago para empresas $1200
Guasap Forensic	Realiza peritajes informáticos de WhatsApp	Versión gratuita limitada.
		Versión pago para empresas $359
Autopsy	Análisis forense informático de sistema de archivos y líneas temporales de ficheros.	Open source
OSForensics	Permite visualizar y obtener información de un escaneo completo al computador	Versión gratuita limitada por 30 días.
		Versión pago $995
Volatility Framework	Análisis de memoria RAM	Open source
Event Log Explorer	Analiza los logs del sistema operativo donde se registran los eventos ejecutados.	Licencia gratuita limitada por 24 horas.
		Versión paga $198 por un año a un equipo
Kali - Linux	Realiza auditorias y seguridad informática a nivel general.	Open source
	TOTAL	**$3201.95**

Nota: Tabla con toda la información de software utilizado en las prácticas.

En base a la Tabla 20 se observa que para implementar un laboratorio con las características que se presentan en este proyecto de titulación es necesario por lo menos un presupuesto de 3200 dólares anuales, que implica el uso de licencias para ciertos programas.

Sin embargo, se considera que también se puede utilizar otras herramientas tanto a nivel de software y hardware, las cuales no se desarrollaron en este proyecto por su alto costo y dificultad para la adquisición, pero se recomienda implementar en el Laboratorio de Informática Forense las cuales se detalla en el siguiente apartado.

3.4 Propuesta para la Adquisición de Hardware y software especializado para el Laboratorio de Informática Forense

A continuación, se tiene una lista de software licenciado o software libre que puede ser adquirido para la implementación del LIF en la Tabla 21.

Tabla 21. Software para análisis forense

Software para análisis forense		
Nombre	**Uso**	**Precio**
EnCase Forensic 8.08	Proceso forense digital Adquisición de datos Evidencia digital Anti-informática forense	Por estación de trabajo $3000 por tres años
Oxygen Detective Forensic	Extracción de información de Android, Apple IOS, Blackberry, Symbian, Windows y otros Smartphone.	Precios de la licencia por un año dependiendo de la versión oscila desde los $452 hasta $1699 por puesto de trabajo
Elcomsoft iOS Forensic Toolkit	Adquisición física y lógica de dispositivos iPhone, iPad y iPod Touch.	Versión completa $1495 por un año.
	TOTAL	**$6194.00**

Nota: Tabla con toda la información de software.

A continuación, se tiene una lista de hardware que puede ser adquirido para la implementación del LIF en la Tabla 22.

Tabla 22. Hardware para análisis forense.

Hardware para análisis forense		
Nombre	**Uso**	**Precio**
Clonador Discos Duros SATA IDE a USB	Clonar la evidencia de manera física para el análisis y así no manipular la evidencia original	$362.28
Wiebetech USB Write Blocker	Para acceder a unidades flash USB o dispositivos que no se pueden eliminar de un puerto USB.	$149
Black Hole Faraday Bag Kit	Aislador de señales de radiofrecuencia para dispositivos móviles y laptops.	$330
Forensic Analysis Workstation	Estación de trabajo completa que nos permite realizar cualquier tipo de análisis ya sea en discos duros o dispositivos móviles, con gran capacidad de procesamiento.	$13500
	TOTAL	**$14341.28**

Nota: Información de hardware.

CONCLUSIONES

- La exploración digital forense es uno de los procesos exiguo estudiados, lo que produce que varios tipos de embestidas informáticas no sean indagados y tratados de forma correcta bajo medidas de resguardo y probidad de la información que se administran conforme a las normativas de ISO 27037:2012.
- La importancia de la investigación forense digital permite adquirir, preservar, obtener información que ha sido procesada y guardada en equipos electrónicos que mediante técnicas y herramientas de extracción de datos se puede obtener evidencia digital probatoria ante procesos judiciales.
- El Centro de Procesamiento de Datos (CPD), tiene la infraestructura necesaria en hardware y software para la ejecución de un Laboratorio de Informática Forense, ya que ofrece las seguridades óptimas para la extracción, preservación y estudio de evidencia digital, manteniendo la seguridad e integridad de la información.
- Con el estudio ejecutado en las diferentes prácticas sobre exploración de computación forense, se puede instituir vías de indagación y con ello resguardar la rectitud de los datos, para que estos logren ser tratados como demostrativos en caso de hallarse una violación informática.
- Cada práctica que tiene este proyecto presenta un conjunto de herramientas que coexisten en el mercado, sean de uso libre como de pago, que consienten efectuar un estudio eficaz de la información entregada como parte de una amenaza informática durante el estudio de la investigación.

RECOMENDACIONES

- Al poseer la infraestructura requerida la Universidad tiene cabida de implementar seminarios o proyectos de educación continua que permitan capacitar a los docentes y estudiantes en temas de investigación, exploración de agresiones informáticas, con un enfoque especial en la informática forense apegadas a las normativas de las leyes ecuatorianas.
- Para la implementación de un Laboratorio de Informática Forense es significativo poseer bien claro el fondo de la seguridad de la información, así como el estudio de los artículos que rigen sobre agresiones informáticas que se encuentran tipificados en código orgánico del Ecuador.
- Dentro del laboratorio de IHM es necesario tener acceso a máquinas virtuales o VDI (Infraestructura de escritorio virtual) con sistemas operativos Windows 10 y Kali Linux, para realizar prácticas de investigación forense, ya que el espacio cuenta con equipos que se pueden utilizar para los análisis de evidencia digital.
- La utilización de herramientas forense es de vital importancia para identificar los hechos que sucedieron durante el ataque realizado, sin embargo, es importante que se cuente con equipos especializados en software y hardware que permitan efectuar un análisis profundo en la extracción de información.
- Al momento de utilizar las herramientas tanto a nivel de hardware como de software es importante mantener actualizadas, esto por el crecimiento exponencial tecnológico que se vive día a día, ya que de igual manera crecen las técnicas de ataques y delitos informáticos.

LISTA DE REFERENCIAS

Academy, N. C. (Octubre de 2018). *Introducción a la Ciberseguridad*. Obtenido de https://static-course-assets.s3.amazonaws.com/CyberSec2.1/es/index.html#1.2.1.3

ADALID. (2015). Obtenido de https://www.adalid.com/

Asamblea Nacional del Ecuador. (Septiembre de 2014). *Código Orgánico Integral Penal. Quito. Ecuador*. Obtenido de https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/95496/112458/F-1546437745/ECU95496.pdf

Ayala, A. M. (Septiembre de 2018). *Lifeder*. Obtenido de https://www.lifeder.com/investigacion-bibliografica/

Bezzi, G. P. (Agosto de 2016). *Análisis de botnets y ataques de denegación de servicio*. Obtenido de Universidad Nacional de la Plata: https://premios.eset-la.com/universitario/pdf/analisis_de_botnets_y_ataques_DDoS.pdf

BynariTI. (2011). Obtenido de http://www.binaryti.com/2012/02/ftk-imager.html

Carlos Quinto Huamán, E. A. (2016). *Análisis de metadatos en vídeos digitales de dispositivos móviles*. Obtenido de http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/666/COMTEL%202016%20-%20Paper23.pdf?sequence=1

Code, M. (Marzo de 2015). *Gestion De Seguridad En Las TIC.* Obtenido de http://mexcodex.blogspot.com/2015/03/111-integridad-disponibilidad-y.html

Colombia, I. F. (2018). Obtenido de https://www.informaticaforense.com.co/la-evidencia-digital/

CursoHacker. (2014). *recuperacion de archivos borrados programas*. Obtenido de http://cursohacker.es/recuperar-archivos-borrados-programas

Diaz, D. (2018). *Universidad Politécnica Salesiana*. Obtenido de http://virtual.ups.edu.ec/presencial52/pluginfile.php/280886/mod_resource/content/0/Cifrado%20y%20confidencialidad%20de%20mensajes.pdf

Digital, C. F. (10 de Julio de 2017). Obtenido de http://ayudasydemascosas.blogspot.com/2017/07/ciencia-forense-digital.html

DMA. (2018). *Departamento de Matemática Aplicada*. Obtenido de http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/criptografia.html

Dona, D. (07 de 2018). *Dispositivos de almacenamiento*. Obtenido de https://www.danieldona.com/informatica%20basica/2%20DISPOSITIVOS%20DE%20ALMACENAMIENTO.pdf

Ecuador, A. N. (10 de Febrero de 2014). *Código Organico Integral Penal*. Obtenido de https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf

Ecuador, P. N. (Septiembre de 2015). Obtenido de http://www.policiaecuador.gob.ec/delitos-informaticos-o-ciberdelitos/

EcuRed. (10 de 2018). Obtenido de https://www.ecured.cu/Inform%C3%A1tica_Forense#Objetivos_de_la_Inform.C3.A1tica_Forense

ESET. (2019). Obtenido de Es una heredero de Peyta ataca al MBR (registro de arranque), si el ataque es efectivo el usuario recibe un mensaje que sus archivos fueron afectados y se encuentran cifrados, para que se pueda recuperar la información el usuario debe cancelar un pago exi

FBI. (2018). *Departamento de Justicia de EE. UU*. Obtenido de https://www.fbi.gov/investigate/cyber

Feandalucia. (Mayo de 2011). *Dirección IP Publica*. Obtenido de https://www.feandalucia.ccoo.es/docu/p5sd7257.pdf

Forense, A. E. (2019). Obtenido de https://imagenforense.es/servicios/analisis-forense-de-imagenes/

Galarreta, R. (1994). *Metodología de la investigación bibliográfica.* Trujillo: En U. P. Orrego.

Gallo, I. P. (s.f.). *Analisis de Correo Electronico*. Obtenido de Researchgate: https://www.researchgate.net/profile/Beatriz_Gallo2/publication/308917364_Pericias_en_Correos_Electronicos/links/57f76ac008ae280dd0bca81c/Pericias-en-Correos-Electronicos.pdf

García Dahinten, C. R. (2014). *biblioteca.usac.edu.gt*. Obtenido de http://biblioteca.usac.edu.gt/tesis/08/08_0755_CS.pdf

Gil, L. M. (2017). *Geolocalización*. Obtenido de http://e-spacio.uned.es/fez/eserv/bibliuned:RDUNED-2017-20-5050/Geolocalizacion.pdf

GitHub. (2019). Obtenido de https://github.com/Quantika14/guasap-whatsapp-foresincs-tool

Gudiño, O. (2 de Febrero de 2017). *Cultura Informática*. Obtenido de https://culturainformatica.co/hacker-crackers-lamers-script-kiddies-phreakers-quienes-son-que-hacen/

Hector Avalos, E. G. (2015). *Seguridad de la información, Generación y Mitigación de un Ataque de Denegación de Servicios*. Obtenido de Revista Tecnológica ESPOL - ISSN 1390-3659: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/425

Hurtado, J. (2010). *Metodología de la Investigación.* Bogota - Caracas: Centro internacional de Estudios Avanzados Sypal y Ediciones Quirón S. A.

Hurtado, J. (25 de Enero de 2015). *Centro Internacional de Estudios Avanzados Sypal*. Obtenido de http://www.cieasypal.com/actividad/investigacion-y-metodologia/como-hacer-investigacion-proyectiva

IMPERVA. (2019). Obtenido de https://www.imperva.com/learn/application-security/high-orbit-ion-cannon/

INCIBE-CERT. (2019). Obtenido de https://www.incibe-cert.es/blog/herramientas-forense-moviles

Información, U. E. (26 de Mayo de 2015). Obtenido de https://www.elmundo.es/sapos-y-princesas/2015/05/26/556425c8ca4741b4698b4575.html

Informática, S. (28 de Diciembre de 2012). Obtenido de http://antisec-security.blogspot.com/2012/12/ataques-dos-ddos-en-seguridad.html

informáticos.mx, D. (2018). Obtenido de https://www.delitosinformaticos.mx/que-es-un-delito-informatico/ciberdelitos-mas-comunes/

INTECO. (Febreo de 2011). Obtenido de https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

Internacional, A. (2019). Obtenido de https://www.ondata.es/recuperar/encase_forensic.htm

Jiménez, J. (01 de 09 de 2018). *Phishing*. Obtenido de https://www.redeszone.net/2018/09/13/asi-evolucionando-ataques-phishing-exito/

LIFE. (2018). Obtenido de https://www.laboratoriodeinformaticaforense.com/index.html

LIGNUX. (s.f.). *https://lignux.com/hoic-hight-orbit-ion-cannon/*.

Mite Villón, J. O., & Sanchez Montero, Y. R. (2016). *Repositorio de la Universidad de Guayaquil*. Obtenido de http://repositorio.ug.edu.ec/bitstream/redug/16749/1/UG-FCMF-B-CINT-PTG-N.110.pdf

MXL. (2019). Obtenido de https://maslinux.es/que-es-kali-gnu-linux/

Nacional, E. P. (2018). Obtenido de https://www.cec-epn.edu.ec/cursos/curso/informatica-forense

Normalización, O. I. (2012). Obtenido de https://www.iso.org/standard/44381.html

Octavio. (11 de Abril de 2017). *kerchak*. Obtenido de https://kerchak.com/que-es-la-informatica-forense/

PassMark. (2019). Obtenido de https://www.osforensics.com/faqs-and-tutorials/mac-linux-drives.html

Paus, L. (08 de 09 de 2016). Obtenido de https://www.welivesecurity.com/la-es/2016/09/08/eventos-de-windows-analisis-forense/

PeritoIT. (2012). Obtenido de https://peritoit.com/2012/10/23/isoiec-270372012-nueva-norma-para-la-recopilacion-de-evidencias/

Proteger mi PC. (Agosto de 2018). Obtenido de https://protegermipc.net/2018/08/23/osforensics-herramienta-informatica-forense-windows/

Pública, S. (2019). Obtenido de https://www.seguridadpublica.es/2013/03/fotoforensics-para-detectar-fotografias-modificadas/

Riofrio, J. F. (2012). *Los Delitos Informáticos y sus tipificación en la Legislación Ecuatoriana*. Obtenido de http://dspace.unl.edu.ec/jspui/bitstream/123456789/9329/1/Jaime%20Francisco%20Riofr%C3%ADo%20.pdf

Rivadeneira, P. (2010). *Derecho. Concepciones Generales. Código penal. Ecuatoriano delito Informático*. Obtenido de http://derechogeneralidades.blogspot.com/2012/09/codigo-penal-ecuatoriano-delitos.html

Rivas, M. (13 de 03 de 2018). *Direcciones IP públicas*. Obtenido de https://www.neoguias.com/direcciones-ip-publicas-todo-lo-que-necesitas-saber/

Rodríguez, F. (2018). *Derecho y cambio Social*. Obtenido de https://www.derechoycambiosocial.com/revista025/informatica_forense.pdf

Ruiz, M. M. (Junio de 2017). *Geolocalizacón*. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64974/6/mmirandaruizTFG0617memoria.pdf

Samaniego, J. F. (Marzo de 2018). *Localizar Direccion IP*. Obtenido de https://www.nobbot.com/pantallas/localizar-una-direccion-ip/

Sanchez, M. G. (11 de Mayo de 2018). Obtenido de https://forojuridico.mx/robo-de-identidad-empresarial-en-medios-digitales/

Stalling, W. (2004). *Person Education*. Obtenido de https://books.google.com.ec/books?id=cjsHVSwbHwoC&pg=PA31&lpg=PA31&dq=INFORMACION+DEL+CRIPTOANALISTA&source=bl&ots=ZozL-5FcKF&sig=-Fk1ZzKLcfO0lT34nC1amfBDA8I&hl=es-419&sa=X&ved=2ahUKEwjikPS1kZPfAhUK0FkKHU4eCpYQ6AEwDXoECAcQAQ#v=onepage&q=INFORMACION%20DEL%

Suárez, J., & Martínez, W. (09 de 2016). *HERRAMIENTAS APLICADAS EN EL DESARROLLO DEL ANÁLISIS FORENSE* . Obtenido de https://repository.unimilitar.edu.co/bitstream/handle/10654/14395/SuarezUrrutiaJenniferCatherine2016.pdf?sequence=1&isAllowed=y

Technologies, A. (s.f.). *PHISING*. Obtenido de https://www.acens.com/wp-content/images/2014/10/wp-phising-acens.pdf

UNAM. (2018). *Investigación bibliográfica* . Obtenido de http://fournier.facmed.unam.mx/deptos/seciss/images/investigacion/12.pdf

Universo, E. (15 de Abril de 2019). Obtenido de https://www.eluniverso.com/noticias/2019/04/15/nota/7287215/ecuador-ha-recibido-40-millones-ataques-ciberneticos-revela

Villalobos, E. (2002). *Diccionario de Derecho Informático.* Panamá: Juridico.

Volatilidad, F. (2018). Obtenido de https://www.volatilityfoundation.org/faq

WELIVESECURITY. (2016). Obtenido de https://www.welivesecurity.com/la-es/2016/12/09/analisis-forense-imagenes-digitales/

Zambrano Mendieta, J., Dueñas Zambrano, K., & Macías Ordoñez, L. (6 de Julio de 2016). *Delito Informático. Procedimiento Penal en Ecuador*. Obtenido de https://dialnet.unirioja.es/descarga/articulo/5761561.pdf