



INSTITUTO TECNOLÓGICO UNIVERSITARIO “RUMIÑAHUI”
CARRERA REDES Y SEGURIDAD INFORMÁTICA.

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA
OBTENCIÓN DEL TÍTULO DE TECNICO SUPERIOR EN
REDES Y SEGURIDAD INFORMÁTICA.

TEMA: ANALISIS, DISEÑO E IMPLEMENTACION DE UN
LABORATORIO DE ANALISIS INFORMATICO FORENSE

AUTORES:

Christian Fernando Fernández Briones Geovanny Mauricio Garófalo
Ángel Iván Duchi Morocho

TUTOR:

Ing. Gerardo Cajamarca

CARTA DE CESIÓN DE DERECHOS DEL TRABAJO DE TITULACIÓN

CT-ANX-2024-ISTER-6-6.1

Sangolquí, 19 de octubre de 2024

MSc. Elizabeth Ordoñez
DIRECTORA DE DOCENCIA

MSc. Mónica Loachamín
COORDINADORA DE TITULACIÓN

**INSTITUTO SUPERIOR TECNOLÓGICO RUMIÑAHUI CON CONDICIÓN DE
UNIVERSITARIO**

Presente

Por medio de la presente, yo ANGEL IVAN DUCHI MOROCHO, declaro y acepto en forma expresa lo siguiente: Ser autor del trabajo de titulación denominado ANALISIS, DISEÑO E IMPLEMENTACION DE UN LABORATORIO DE ANALISIS INFORMATICO FORENSE , de la Tecnicatura Superior REDES Y SEGURIDAD INFORMATICA; y a su vez manifiesto mi voluntad de ceder al Instituto Superior Tecnológico Rumiñahui con condición de Universitario, los derechos de reproducción, distribución y publicación de dicho trabajo de titulación, en cualquier formato y medio, con fines académicos y de investigación.

Esta cesión se otorga de manera no exclusiva y por un periodo indeterminado. Sin embargo, conservo los derechos morales sobre mi obra.

En fe de lo cual, firmo la presente.

Atentamente,



ANGEL IVAN DUCHI MUROCHO
C.I.: 0605544766

CARTA DE CESIÓN DE DERECHOS DEL TRABAJO DE TITULACIÓN

CT-ANX-2024-ISTER-6-6.1

Sangolquí, 24 de Octubre del 2024

MSc. Elizabeth Ordoñez
DIRECTORA DE DOCENCIA

MSc. Mónica Loachamín
COORDINADORA DE TITULACIÓN

**INSTITUTO SUPERIOR TECNOLÓGICO RUMIÑAHUI CON CONDICIÓN DE
UNIVERSITARIO**

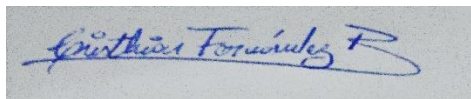
Presente

Por medio de la presente, yo, **CHRISTIAN FERNANDO FERNANDEZ BRIONES** declaro y acepto en forma expresa lo siguiente: Ser autor del trabajo de titulación denominado **ANALISIS DISEÑO E IMPLEMENTACION DE UN LABORATORIO DE ANALISIS INFORMATICO FORENSE**, de la Tecnicatura Superior EN REDES Y SEGURIDAD INFORMÁTICA; y a su vez manifiesto mi voluntad de ceder al Instituto Superior Tecnológico Rumiñahui con condición de Universitario, los derechos de reproducción, distribución y publicación de dicho trabajo de titulación, en cualquier formato y medio, con fines académicos y de investigación.

Esta cesión se otorga de manera no exclusiva y por un periodo indeterminado. Sin embargo, conservo los derechos morales sobre mi obra.

En fe de lo cual, firmo la presente.

Atentamente,



CHRISTIAN FERNANDO FERNANDEZ BRIONES
C.I.: 1204709677

FORMULARIO PARA ENTREGA DE PROYECTOS EN BIBLIOTECA INSTITUTO SUPERIOR TECNOLÓGICO RUMIÑAHUI CON CONDICIÓN DE UNIVERSITARIO

CT-ANX-2024-ISTER-1

CARRERA:

TECNICO SUPERIOR EN REDES Y SEGURIDAD INFORMATICA

AUTOR /ES:

CRISTIAN FERNANDO FERNANDEZ BRIONES.

GEOVANNY MAURICIO GAROFALO.

ANGEL IVAN DUCHI MOROCHO.

TUTOR:

CAJAMARCA MÉMDEZ GERARD IVÁN

CONTACTO ESTUDIANTE:

0985876056

CORREO ELECTRÓNICO:

Angeldmc9622@gmail.com

TEMA:

ANALISIS, DISEÑO E IMPLEMENTACION DE UN LABORATORIO DE ANALIS
INFORMATICO FORENCE.

OPCIÓN DE TITULACIÓN:

REDES Y SEGURIDAD INFORMATICA

RESUMEN EN ESPAÑOL:

EL ANÁLISIS DISEÑO E IMPLEMENTACIÓN DE UN LABORATORIO DE ANALISIS
INFORMATICO FORENCE SE ENFOCA EN TÉCNICAS AVANZADAZ PARA LA
RECOLECCION, ANALISIS Y PERSERVACIONDE EVIDENCIAS DIGITALES. Y
NOS PERMITIRA RECUPERAR DATOS OCULTOS O ELIMINADO, TAMBIEN NOS
PERMITIRA ANALIZAR REDES COMPROMETIDAS Y DESCUBRIR TRAZAS DE
ACTIVIDADES ILISITAS EN DISPOSITIVOS ELECTRONICOS.

ESTE PROYECTO BUSCA CREAR ESA BRECHAS, ESTABLECIENDO ESTE
LABORATORIO DE ANALISIS FORENSE INFORMATICO QUE OFRECA UNA
FORMACION INTEGRAL EN LA INVESTIGACION DE DELITOS CIBERNETICOS.

PALABRAS CLAVE:

(DISPOSITIVOS ELECTRONICOS, ANALISIS, EVIDENCIA DIGITAL, DATOS,
REDES, DELITOS CIBERNETICOS)

FORMULARIO PARA ENTREGA DE PROYECTOS EN BIBLIOTECA INSTITUTO SUPERIOR TECNOLÓGICO RUMIÑAHUI CON CONDICIÓN DE UNIVERSITARIO

CT-ANX-2024-ISTER-1

CARRERA:

TECNICO SUPERIOR EN REDES Y SEGURIDAD INFORMATICA

AUTOR /ES:

(CHRISTIAN FERNANDO FERNANDEZ BRIONES, ANGEL IVAN DUCHI
MOROCHO, GEOVANNY MAURICIO GAROFALO CRUZ)

TUTOR:

CAJAMARCA MÉNDEZ GERARDO IVÁN

CONTACTO ESTUDIANTE:

0991110061

CORREO ELECTRÓNICO:

christian.fernandez@ister.edu.ec

TEMA:

ANALISIS DISEÑO E IMPLEMENTACION DE UN LABORATORIO DE ANALISIS
INFORMATICO FORENSE.

OPCIÓN DE TITULACIÓN:

REDES Y SEGURIDAD INFORMATICA

RESUMEN EN ESPAÑOL:

Este trabajo presenta el análisis, diseño e implementación de un laboratorio de análisis informático forense en el Instituto Tecnológico Superior Rumiñahui. Se identificaron las necesidades tecnológicas, se diseñaron los espacios y herramientas requeridas, y se implementaron procedimientos basados en normas internacionales para la recolección y análisis de evidencia digital. El laboratorio fue probado con escenarios reales, demostrando su utilidad en la formación de expertos y en el apoyo a investigaciones forenses.

ANALISIS

Se evaluaron las necesidades tecnológicas y operativas para implementar un laboratorio forense en el Instituto Tecnológico Superior Rumiñahui. Se analizaron herramientas forenses, infraestructura y normativas, enfocándose en garantizar la recolección y análisis de evidencia digital de manera confiable y segura. El estudio permitió definir los recursos y procedimientos necesarios para un laboratorio funcional y acorde a los estándares internacionales.

DISEÑO

El diseño del laboratorio de análisis informático forense en el Instituto Tecnológico Superior Rumiñahui se enfocó en crear un espacio seguro y eficiente para la recolección y análisis de evidencia digital. Para ello, se establecieron los requisitos técnicos, incluyendo software especializado, hardware de alto rendimiento y medidas de seguridad tanto física como digital. Se configuró el espacio físico con áreas separadas para el almacenamiento de evidencia, análisis de datos y capacitación del personal.

Además, se definieron protocolos y flujos de trabajo que aseguran la integridad de la evidencia y la eficiencia de los procesos. Este diseño garantiza que el laboratorio cumpla con las normativas internacionales, permitiendo a los estudiantes y profesionales realizar análisis forenses de alta calidad.

IMPLEMENTACION

La implementación del laboratorio forense en el Instituto Tecnológico Superior Rumiñahui incluyó la instalación y configuración de herramientas especializadas para el análisis digital, así como la disposición del hardware y software necesarios para realizar investigaciones forenses. Se establecieron controles de seguridad física y digital para proteger la evidencia y se instalaron sistemas de respaldo de datos.

Finalmente, se realizaron pruebas en escenarios simulados para asegurar el funcionamiento efectivo del laboratorio, verificando su capacidad para soportar investigaciones de manera confiable y cumpliendo con estándares internacionales.

PALABRAS CLAVE:

- Análisis forense informático
- Laboratorio forense
- Evidencia digital
- Seguridad informática
- Implementación de laboratorio
- Normativas internacionales
- Recolección y análisis de datos
- Protocolo de manejo de evidencia

ABSTRACT:

This project presents the analysis, design, and implementation of a digital forensic analysis laboratory at Instituto Tecnológico Superior Rumiñahui, aiming to provide a specialized and reliable environment for the identification, preservation, analysis, and presentation of digital evidence in judicial investigations. The project begins with an assessment of technological and procedural needs, addressing key aspects such as data integrity, security measures, and compliance with international forensic standards.

In the design phase, specific technical requirements, including hardware, specialized software, and secure physical infrastructure, were identified to ensure a controlled environment for forensic work. The implementation involved selecting and configuring appropriate forensic tools, establishing clear protocols for handling digital evidence, and training personnel to maintain high operational standards. These measures facilitate reliable digital investigations and allow the laboratory to function as both a professional and educational resource.

Finally, the laboratory's effectiveness was evaluated through practical tests using simulated forensic scenarios, confirming its capacity to support accurate and timely forensic analyses. This project provides an effective model for implementing digital forensic labs in academic settings, enhancing regional capabilities in digital forensics and contributing to the field of digital justice.

PALABRAS CLAVE:

- Digital forensics
- Forensic laboratory
- Digital evidence
- Cybersecurity
- International standards

SOLICITUD DE PUBLICACIÓN DEL TRABAJO DE TITULACIÓN

CT-ANX-2024-ISTER-2
Sangolquí, 19 de octubre del 2024

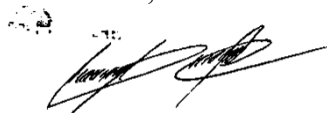
Sres.-

**INSTITUTO SUPERIOR TECNOLÓGICO RUMIÑAHUI CON CONDICIÓN DE
UNIVERSITARIO**

Presente

A través del presente me permito aceptar la publicación del trabajo de titulación de la Unidad de Integración Curricular en el repositorio digital “DsPace” del estudiante: ANGEL IVAN DUCHI MOROCHO, con C.I.: 0605544766 alumno de la Carrera TECNICO SUPERIOR EN REDES Y SEGURIDAD INFORMATICA.

Atentamente,



Firma del Estudiante
C.I.: 0605544766

SÓLO PARA USO DEL ISTER

Han sido revisadas las similitudes del trabajo en el software “TURNITING” y cuenta con un porcentaje de; motivo por el cual, el Proyecto Técnico de Titulación es publicable. (EL PORCENTAJE DE SIMILITUD DEBE SER MÁXIMO DE 15%)

MSc. Elizabeth Ordoñez
DIRECTORA DE DOCENCIA

MSc. Mónica Loachamín
COORDINADORA DE TITULACIÓN

Fecha del Informe ____/____/____

SOLICITUD DE PUBLICACIÓN DEL TRABAJO DE TITULACIÓN

CT-ANX-2024-ISTER-2
Sangolquí, (día) de (mes) del 2024

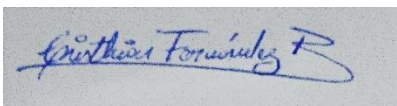
Sres.-

**INSTITUTO SUPERIOR TECNOLÓGICO RUMIÑAHUI CON CONDICIÓN DE
UNIVERSITARIO**

Presente

A través del presente me permito aceptar la publicación del trabajo de titulación de la Unidad de Integración Curricular en el repositorio digital “DsPace” del estudiante: FERNANDEZ BRIONES CHRISTIAN FERNANDO, con C.I.: 1204709677 alumno de la Carrera TECNICO SUPERIOR EN REDES Y SEGURIDAD INFORMATICA.

Atentamente,



Firma del Estudiante
C.I.: 1204709677

SÓLO PARA USO DEL ISTER

Han sido revisadas las similitudes del trabajo en el software “TURNITING” y cuenta con un porcentaje de; motivo por el cual, el Proyecto Técnico de Titulación es publicable. (EL PORCENTAJE DE SIMILITUD DEBE SER MÁXIMO DE 15%)

MSc. Elizabeth Ordoñez
DIRECTORA DE DOCENCIA

MSc. Mónica Loachamín
COORDINADORA DE TITULACIÓN

Fecha del Informe ____ / ____ / ____

MATRIZ SANGOLQUÍ: Av. Atahualpa 1701 y 8 de Febrero

Telf: 0960052734 / 023524576 / 022331628

 www.ister.edu.ec / info@ister.edu.ec

Agradecimiento:**Christian Fernando Fernández Briones:**

Quiero expresar mi más profundo agradecimiento a mi esposa Yanira Parrales Mera, cuyo amor, apoyo y comprensión incondicionales han sido mi mayor fuente de inspiración y fortaleza a lo largo de este camino. Sin su paciencia y aliento constante, este logro no hubiera sido posible.

A mis hijos, quienes me llenan de alegría y motivación cada día. Su sonrisa y energía han sido un recordatorio constante de la importancia de este esfuerzo y del ejemplo que quiero darles.

A mi familia, por su apoyo incondicional y por estar siempre a mi lado, brindándome el aliento necesario para seguir adelante. Sus palabras de aliento y su confianza en mis capacidades han sido fundamentales para alcanzar esta meta.

Gracias a todos por creer en mí y por ser una parte esencial de este logro.

Geovanny Mauricio Garófalo:

Mis agradecimientos van dirigidos hacia mi familia, especialmente mis padres.

Ángel Iván Duchi Morocho:

Agradecer a mis amigos y compañeros que han estado a mi lado en este viaje académico, ofreciendo su aliento y motivación. Finalmente, a mis profesores, cuyo conocimiento y dedicación han sido fundamentales para alcanzar este logro. Esta tesis es el resultado de su inquebrantable apoyo y guía. Gracias a todos por ser parte de este logro tan significativo.

Dedicatoria**Christian Fernando Fernández Briones:**

Dedico esta tesis con todo mi corazón a mi amada esposa, Yanira Parrales Mera, cuyo amor, comprensión y apoyo incondicional me han dado la fuerza para superar cada desafío

en el camino. Su fe en mí y en mi capacidad ha sido la fuente de mi perseverancia y éxito, y no podría haber alcanzado este logro sin su presencia constante y alentadora.

A mis hijos Hansel, Elkin, Ibrahim, quienes son la razón de mi esfuerzo y dedicación. Su alegría y entusiasmo han sido una inspiración diaria para mí. Esta tesis es un testimonio de mi amor por ustedes y de mi compromiso para ofrecerles un futuro lleno de oportunidades y aprendizaje.

Y a mi familia, que siempre ha estado a mi lado, brindándome el apoyo emocional y moral que tanto he necesitado. Cada miembro de mi familia ha jugado un papel crucial en este viaje, y su amor y paciencia han sido el pilar de mi fortaleza.

A todos ustedes, mi gratitud eterna. Este logro es tanto mío como de ustedes, y es un reflejo de los sacrificios y la dedicación compartidos. Gracias por ser mi mayor fuente de inspiración y apoyo en cada paso de este camino.

Geovanny Mauricio Garófalo:

Dedico esta tesis a mi familia, especialmente mis padres.

Ángel Iván Duchi Morocho:

Dedico esta tesis a mis padres, quienes siempre me han brindado su amor incondicional, apoyo y sabiduría a lo largo de mi vida. Su confianza en mis capacidades ha sido una fuente constante de inspiración.

INDICE

1. Antecedentes.....	5
2. Problema.....	6
3. Objetivos.....	7
2.1. Objetivo General:	7
2.2. Objetivos Específicos:	7
4. Justificación	7
4.1. Justificación Legal:.....	8
4.2. Justificación Social:.....	8
4.3. Justificación Técnica:	8
4.4. Justificación Académica:	8
5. Marco Teórico	9
5.1 Informática Forense	9
5.2 Normativas y Estándares en Informática Forense	9
5.4 Herramientas de Análisis Forense	10
5.5 Diseño e Implementación de un Laboratorio Forense.....	11
5.6 Retos y Consideraciones Éticas	11
6. Alcance y Resultados Esperados	12
6.1. Identificación de Requisitos:	12
6.2. Adquisición de Herramientas:	12
6.3. Desarrollo de Procedimientos Operativos:	12
6.4. Implementación y Validación:.....	12
7. Impacto y Beneficiarios Impacto:	14
8. Conclusiones.....	16
9. Recomendaciones	17
10. Bibliografía	19

1. Antecedentes

El análisis informático forense ha emergido como una herramienta clave para combatir los delitos cibernéticos en todo el mundo. Con el incremento exponencial de las actividades delictivas digitales, como el fraude en línea, el robo de identidad y los ataques de hacking, se ha vuelto indispensable el uso de técnicas avanzadas para la recolección, análisis y preservación de evidencia digital. Esta disciplina permite recuperar datos ocultos o eliminados, analizar redes comprometidas y descubrir trazas de actividad ilícita en dispositivos electrónicos.

En Ecuador, instituciones educativas como el Instituto Tecnológico Superior Rumiñahui (ISTER) enfrentan un desafío particular: la falta de infraestructura adecuada para formar a los estudiantes en las competencias necesarias para enfrentar los desafíos de la informática forense. Actualmente, el ISTER no cuenta con un laboratorio especializado, lo que limita tanto la enseñanza teórica como la práctica. Esto afecta la capacidad del instituto para preparar a futuros profesionales en análisis forense digital, una disciplina que sigue siendo relativamente nueva en el contexto académico local.

Este proyecto busca cerrar esa brecha, estableciendo un laboratorio de análisis forense informático en el ISTER que se alinee con los estándares internacionales y que ofrezca una formación integral en la investigación de delitos cibernéticos

2. Problema

El Instituto Tecnológico Superior Rumiñahui (ISTER) enfrenta la necesidad urgente de contar con un laboratorio especializado en análisis forense informático. Actualmente, no dispone de las herramientas ni la infraestructura necesaria para formar adecuadamente a sus estudiantes en este campo crucial. Las principales deficiencias son:

- Falta de Equipos y Herramientas Especializadas: El ISTER no cuenta con estaciones de trabajo forense, duplicadoras de discos, ni software licenciado para realizar análisis forense informático, limitando así la capacidad de enseñanza práctica y precisa.
- Ausencia de Procedimientos Estandarizados: El instituto no dispone de protocolos operativos ajustados a normativas internacionales como el ISO/IEC 27037, lo que dificulta la enseñanza de prácticas correctas de manejo y preservación de evidencia digital.
- Cumplimiento Legal y Académico: Sin un laboratorio adecuado, el ISTER no puede cumplir con las normativas legales del Código Orgánico Integral Penal (COIP) ni con los estándares educativos de calidad requeridos para una formación competente en informática forense.
- Deficiencia en Capacitación: La falta de un espacio adecuado y herramientas específicas impide que el ISTER ofrezca formación técnica avanzada, limitando las competencias

profesionales de sus estudiantes en análisis forense digital y afectando su preparación para el mercado laboral.

3. Objetivos

2.1. Objetivo General:

Diseñar e implementar un laboratorio de análisis informático forense en el Instituto Tecnológico Superior Rumiñahui, que cumpla con los estándares internacionales de calidad, garantizando precisión, seguridad y validez en la recolección y análisis de evidencia digital.

2.2. Objetivos Específicos:

- Evaluar las necesidades específicas del laboratorio en función de los tipos de análisis forense requeridos, como la recuperación de datos y el análisis de redes, enfocado en las actividades formativas y de investigación del instituto.
- Desarrollar un diseño físico y lógico que contemple la disposición óptima de los equipos, la configuración de la red, y las medidas de seguridad necesarias para proteger la integridad de las pruebas y el entorno operativo.
- Seleccionar y configurar el hardware y software forense especializado, asegurando que su uso sea eficiente y esté alineado con los estándares internacionales como ISO/IEC 27037.
- Establecer procedimientos operativos claros para la adquisición, preservación y análisis de evidencia digital, garantizando el cumplimiento de las normativas legales vigentes y los estándares forenses internacionales.
- Implementar y probar el laboratorio, verificando que todos los componentes cumplan con los requisitos operacionales y técnicos, asegurando su correcto funcionamiento antes de su uso académico y profesional.

4. Justificación

4.1. Justificación Legal:

La implementación del laboratorio de análisis forense informático en el Instituto Tecnológico Superior Rumiñahui permitirá que la institución se ajuste a los marcos legales nacionales e internacionales en el manejo de evidencia digital. Esto asegurará que las pruebas recogidas sean válidas ante los tribunales, protegiendo el derecho al debido proceso. La creación del laboratorio permitirá cumplir con estándares como el ISO/IEC 27037:2012, garantizando la correcta recolección y preservación de la evidencia digital, fortaleciendo así el respaldo jurídico de la institución.

4.2. Justificación Social:

La creación de este laboratorio en el Instituto reforzará las capacidades de investigación y resolución de crímenes digitales en la región, mejorando la seguridad cibernética. También fortalecerá la relación de confianza entre la sociedad y las instituciones al promover la formación de especialistas que contribuyan a la seguridad y privacidad digital de la comunidad. Como parte de una institución educativa, el laboratorio servirá para preparar a los futuros profesionales encargados de proteger la información y combatir delitos tecnológicos.

Ñ

4.3. Justificación Técnica:

El laboratorio ofrecerá acceso a herramientas especializadas y avanzadas que permitirán realizar investigaciones forenses de alta precisión, tales como la recuperación de datos y el análisis de redes y sistemas informáticos. La implementación de estas tecnologías en el Instituto Tecnológico Superior Rumiñahui garantizará que los estudiantes y el personal puedan realizar análisis técnicos complejos, mejorando la calidad y eficacia de las investigaciones.

4.4. Justificación Académica:

La implementación del laboratorio en el Instituto Tecnológico Superior Rumiñahui proporcionará a los estudiantes una plataforma educativa innovadora para la formación en informática forense. Este recurso permitirá a los alumnos adquirir experiencia práctica y realizar investigaciones académicas con acceso a herramientas de última generación. La

integración del laboratorio fortalecerá la enseñanza en este campo, posicionando al Instituto como líder en la capacitación y formación de expertos en forense digital.

5. Marco Teórico

5.1 Informática Forense

Definición y Alcance:

La informática forense es una rama de la ciberseguridad que se dedica a la identificación, recolección, preservación, análisis y presentación de evidencia digital de manera que pueda ser admisible en un proceso legal. Esta disciplina abarca el análisis de computadoras, redes, dispositivos móviles, y otros medios digitales relevantes. En Ecuador, la aplicación de la informática forense es fundamental para enfrentar delitos cibernéticos y garantizar la justicia a través de pruebas digitales verificables (Casey, 2011).

Evolución Histórica:

Desde los años 80, cuando la informática forense se centraba en la recuperación de datos básicos, ha evolucionado para hacer frente a nuevas amenazas digitales, como el hacking avanzado y la explotación de vulnerabilidades en redes. Este crecimiento ha acompañado la expansión de la tecnología digital y su impacto en la vida cotidiana (Salomon, 2019).

Áreas de Aplicación:

- Investigación Criminal: La informática forense es clave para investigaciones en casos de fraude, robo de identidad y delitos cibernéticos (Carrier, 2005).
- Seguridad de la Información: Identificación de brechas de seguridad e incidentes como la filtración de datos (Casey, 2011).
- Auditorías y Cumplimiento: Verificación del cumplimiento normativo dentro de organizaciones (Carrier, 2005).

5.2 Normativas y Estándares en Informática Forense

ISO/IEC 27037:2012:

Esta norma establece directrices para la identificación, adquisición, y preservación de evidencia digital. Su cumplimiento es fundamental para asegurar que los procedimientos forenses sean válidos y se mantenga la integridad de la evidencia durante todo el proceso legal (ISO, 2012).

NIST SP 800-86:

Esta guía del NIST proporciona un marco para la integración de técnicas forenses en la respuesta a incidentes de seguridad informática, un estándar de gran relevancia en la configuración de laboratorios forenses (Kent, 2006).

Código Orgánico Integral Penal (COIP):

En Ecuador, el COIP establece las bases legales para el manejo de pruebas digitales en investigaciones criminales, asegurando que cualquier evidencia recolectada cumpla con los requisitos legales (Salomon, 2019).

5.3 Metodologías de Análisis Forense

Modelo de Ciclo de Vida del Análisis Forense:

Este modelo describe las fases clave de un proceso forense, desde la identificación de evidencia hasta la presentación de los resultados. Las etapas incluyen:

- Identificación: Localización de fuentes de evidencia digital.
- Recolección: Adquisición de datos preservando su integridad.
- Análisis: Evaluación detallada de los datos.
- Preservación: Almacenamiento seguro de las evidencias.
- Presentación: Preparación de informes para procesos judiciales (Casey, 2011).

5.4 Herramientas de Análisis Forense

Herramientas Comerciales:

- EnCase: Plataforma robusta que permite la recolección y análisis de datos digitales de forma eficiente (Casey, 2011).
- FTK (Forensic Toolkit): Ofrece una solución integral para el análisis forense y recuperación de archivos eliminados (Salomon, 2019).

Herramientas de Código Abierto:

- Autopsy/Sleuth Kit: Solución gratuita y abierta para análisis de discos y grandes volúmenes de datos (Carrier, 2005).
- Wireshark: Herramienta popular para el análisis de tráfico de red en tiempo real (Kent, 2006).

5.5 Diseño e Implementación de un Laboratorio Forense

Requerimientos de Infraestructura:

Para implementar un laboratorio forense en el Instituto Tecnológico Superior Rumiñahui (ISTER), es necesario contar con estaciones de trabajo de alto rendimiento, almacenamiento seguro y redes segmentadas. Esto garantizará que los análisis se realicen sin riesgo de alteración de los datos (Casey, 2011).

Políticas y Procedimientos:

- Protocolos de Adquisición de Evidencia: Establecer procedimientos que aseguren la correcta manipulación de la evidencia digital (ISO, 2012).
- Procedimientos de Análisis: Implementar metodologías estandarizadas para asegurar la consistencia y repetibilidad en los análisis forenses (ISO, 2012).

Capacitación del Personal:

El personal del laboratorio debe estar continuamente capacitado en las últimas técnicas y herramientas forenses, así como en el manejo de evidencia según las normativas vigentes (Salomon, 2019).

5.6 Retos y Consideraciones Éticas

Desafíos Técnicos:

El rápido avance de la tecnología, como la adopción del cifrado y la computación en la nube, presenta desafíos constantes para los profesionales forenses que necesitan adaptarse a nuevas amenazas tecnológicas (Carrier, 2005).

Consideraciones Éticas:

Es esencial que el análisis forense se realice con integridad, respetando la privacidad de las personas involucradas y evitando la manipulación indebida de la información obtenida durante las investigaciones (Casey, 2011).

6. Alcance y Resultados Esperados

6.1. Identificación de Requisitos:

El alcance del proyecto incluye la identificación y adquisición de los siguientes requisitos para establecer un laboratorio de análisis forense informático en el Instituto:

- Hardware:

- Estación de Trabajo Forense (alta capacidad de procesamiento y almacenamiento).
- Duplicadora de Discos Forenses (para garantizar la integridad de la evidencia).
- Dispositivos de Almacenamiento Externo (para la preservación segura de datos).

- Software:

- Herramientas de Análisis Forense (como EnCase o FTK).
- Programas de Duplicación de Datos (como FTK Imager).
- Aplicaciones de Documentación y Reporte (para registrar procedimientos y resultados).

6.2. Adquisición de Herramientas:

El proyecto contempla la adquisición del hardware y software necesario para la funcionalidad del laboratorio. Esto incluye la selección de proveedores confiables y la obtención de licencias de software.

6.3. Desarrollo de Procedimientos Operativos:

Se establecerán procedimientos claros para la adquisición, preservación y análisis de evidencias digitales, asegurando que cumplan con las normativas locales y estándares internacionales.

6.4. Implementación y Validación:

La implementación del laboratorio incluirá:

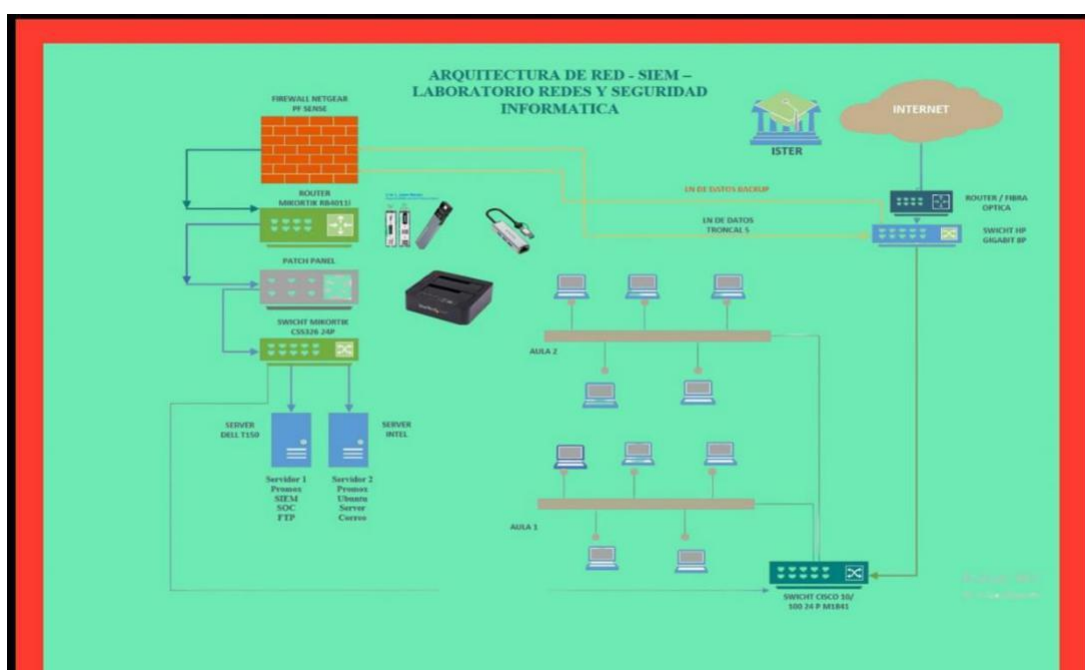
- Instalación y configuración del equipo y software.

- Validación del funcionamiento del laboratorio mediante pruebas y auditorías.

- Generación de informes sobre el estado de la implementación y ajuste de procedimientos según sea necesario.

Resultados Esperados:

- Un laboratorio funcional y equipados adecuadamente para la investigación forense digital.
- Personal capacitado que pueda llevar a cabo análisis forenses de acuerdo con las mejores prácticas.
- Procedimientos operativos que aseguren la integridad y validez de la evidencia digital.
- Contribución al fortalecimiento de la educación y la investigación en informática forense dentro del Instituto.



7. Impacto y Beneficiarios Impacto:

- Eficiencia en la Investigación:

El laboratorio mejorará la velocidad y precisión en la investigación de delitos informáticos, permitiendo un análisis forense detallado y eficiente, lo que agilizará la resolución de casos y la recolección de evidencia crítica.

- Cumplimiento Legal:

El laboratorio garantizará que las pruebas digitales se manejen bajo los lineamientos del Código Orgánico Integral Penal (COIP) y otras normativas, asegurando la validez y protección de la cadena de custodia para su uso en procedimientos judiciales.

- Desarrollo Profesional:

La capacitación en análisis forense dotará a los profesionales de habilidades especializadas, fortaleciendo sus competencias técnicas y fomentando su crecimiento en un campo con alta demanda de expertos.

Beneficiarios Directos:**- Estudiantes del ISTER:**

Los alumnos del programa de Redes y Seguridad Informática podrán realizar prácticas con equipos y software especializados, adquiriendo competencias clave en análisis forense digital y seguridad informática, preparándolos para el entorno laboral.

- Docentes y Personal Técnico del ISTER:

Los docentes utilizarán el laboratorio como recurso educativo, guiando a los estudiantes en actividades prácticas. Además, el personal técnico tendrá acceso a un espacio adecuado para investigación y desarrollo de nuevas técnicas de seguridad digital.

Beneficiarios Indirectos:**- Otras Organizaciones:**

Empresas e instituciones públicas que colaboren con el laboratorio se beneficiarán de sus capacidades para investigaciones forenses y la mejora de la seguridad digital en sus entornos.

- Comunidades Locales:

La capacidad mejorada para combatir crímenes cibernéticos contribuirá a una mayor seguridad digital en la región, reduciendo el impacto de delitos informáticos y fomentando la confianza en las instituciones.

- **Sistema Judicial:**

El laboratorio proporcionará al sistema judicial pruebas digitales confiables, facilitando el manejo adecuado de casos de delitos informáticos y contribuyendo a una administración de justicia más efectiva.

8. Conclusiones

La implementación de un laboratorio de análisis informático forense en el Instituto Tecnológico Superior Rumiñahui (ISTER) representa un avance significativo en la consolidación de las capacidades tecnológicas y educativas de la institución. Los principales puntos que se destacan son:

- **Fortalecimiento Académico:** El laboratorio proporcionará un entorno práctico en el que los estudiantes de la carrera de Redes y Seguridad Informática podrán aplicar conocimientos teóricos, mejorando así su formación técnica y profesional. Además, permitirá al personal docente impartir conocimientos avanzados de análisis forense digital, elevando el nivel académico general del ISTER.

- **Cumplimiento de Normativas:** La infraestructura del laboratorio, junto con los procedimientos estandarizados implementados, asegura que las actividades del mismo cumplan con las normativas legales vigentes, como el Código Orgánico Integral Penal (COIP), y estándares internacionales como ISO/IEC 27037. Esto garantiza que tanto estudiantes como docentes trabajen en un entorno ajustado a los requerimientos técnicos y legales actuales.

- **Innovación Educativa:** El ISTER se consolidará como una institución líder en el ámbito de la informática forense, diferenciándose de otras instituciones a nivel nacional. El acceso a un entorno de análisis forense digital de última generación le brindará a sus estudiantes una ventaja

competitiva al simular situaciones reales de investigación y análisis digital, preparándolos para los desafíos del mercado laboral.

9. Recomendaciones

Para asegurar el éxito y la continuidad del laboratorio, se presentan las siguientes recomendaciones:

1. Capacitación Continua del Personal: Se sugiere implementar un programa permanente de capacitación para docentes y técnicos del laboratorio, enfocándose en las últimas herramientas y metodologías de análisis forense. Además, se recomienda la obtención de certificaciones internacionales reconocidas en el ámbito forense para mantener al personal actualizado.

2. Actualización Tecnológica: Es fundamental planificar la renovación periódica de equipos y software, aproximadamente cada 3 a 5 años, para garantizar que el laboratorio mantenga su alineación con los avances tecnológicos y continúe cumpliendo con los estándares internacionales de calidad.

3. Integración en el Plan de Estudios: El laboratorio debe integrarse de manera transversal en el currículo de la carrera de Redes y Seguridad Informática, permitiendo a los estudiantes realizar prácticas regulares y proyectos finales centrados en el análisis forense digital. Esto fortalecerá su aprendizaje práctico y los preparará mejor para su futura vida profesional.

4. Colaboración Interinstitucional: Se recomienda establecer acuerdos de cooperación con otras instituciones educativas, empresas, y entidades gubernamentales para utilizar el laboratorio en proyectos conjuntos, investigaciones colaborativas y programas de capacitación externa. Esto incrementará la relevancia y el impacto del laboratorio, expandiendo sus beneficios más allá de los estudiantes del ISTER.

Estas conclusiones y recomendaciones están diseñadas para maximizar el impacto del laboratorio forense en el ISTER, no solo mejorando la formación de los estudiantes, sino también consolidando a la institución como un referente en el análisis forense digital en la región.

10. Bibliografía

- Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Elsevier Academic Press.
- Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional.
- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response (NIST SP 800-86). National Institute of Standards and Technology (NIST).
- Salomon, D. (2019). Foundations of Computer Security (2nd ed.). Springer.
- ISO/IEC 27037:2012. (2012). Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence. International Organization for Standardization.
- Código Orgánico Integral Penal (COIP) – Ecuador. (2014). Asamblea Nacional del Ecuador.
[Disponible en línea](<https://www.asambleanacional.gob.ec/sites/default/files/documents/old/definiciones/pdfs/coip.pdf>).
- Bunting, S., & Wei, W. (2013). The Official EnCase Certified Examiner Study Guide. John Wiley & Sons.
- Kruse, W. G., & Heiser, J. G. (2001). Computer Forensics: Incident Response Essentials. Addison-Wesley Professional.
- Nelson, B., Phillips, A., & Steuart, C. (2014). Guide to Computer Forensics and Investigations. Cengage Learning.
- Soltani, S. (2016). Computer Forensics: A Beginner's Guide. McGraw-Hill Education.

- Sammons, J. (2012). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Syngress.

- Noblett, M., Pollitt, M. & Presley, L. (2000). Recovering and Examining Computer Forensic Evidence. Forensic Science Communications, Federal Bureau of Investigation.
- Altheide, C., & Carvey, H. (2011). Digital Forensics with Open Source Tools. Syngress.
- NIST SP 800-88 Rev. 1. (2014). Guidelines for Media Sanitization. National Institute of Standards and Technology.
- Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence, 1(3).
- Bejtlich, R. (2004). The Tao of Network Security Monitoring: Beyond Intrusion Detection. Addison-Wesley.
- Whitman, M. E., & Mattord, H. J. (2017). Principles of Information Security. Cengage Learning.
- Eoghan, C. (2004). Forensic Discovery. Addison-Wesley.
- IEEE 829-2008. Standard for Software and System Test Documentation. Institute of Electrical and Electronics Engineers.

