UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS

MARCO DE TRABAJO Y HERRAMIENTAS PARA EL ANÁLISIS FORENSE EN LA ATENCIÓN DE LOS DELITOS INFORMÁTICOS DE CIBERGROOMING BAJO LOS DISPOSITIVOS MÓVILES ANDROID.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL

TÍTULO DE INGENIERO DE SISTEMAS

AUTOR: MISAEL JULIO MURUDUMBAY HUERTA

DIRECTOR: ING. CRISTINA FLORES URGILES

CAÑAR - ECUADOR

2022

DIOS, PATRIA, CULTURA Y DESARROLLO

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE TECNOLOGÍAS DE LA INFORMACION Y COMUNICACIÓN

CARRERA DE SISTEMAS

MARCO DE TRABAJO Y HERRAMIENTAS PARA EL ANÁLISIS FORENSE EN LA ATENCIÓN DE LOS DELITOS INFORMÁTICOS DE CIBERGROOMING BAJO LOS DISPOSITIVOS MÓVILES ANDROID.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL

TÍTULO DE INGENIERO EN SISTEMAS

AUTOR: MISAEL JULIO MURUDUMBAY HUERTA

DIRECTOR: ING. CRISTINA FLORES URGILES

CAÑAR - ECUADOR

2022

DIOS, PATRIA, CULTURA Y DESARROLLO

Declaratoria de Autoría y Responsabilidad

Misael Julio Murudumbay Huerta portador(a) de la cédula de ciudadanía Nº **0350160487**. Declaro ser el autor de la obra: "**Marco de Trabajo y Herramientas para el Análisis Forense en la atención de los delitos Informáticos de Cibergrooming bajo los dispositivos móviles Android."**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, **18 de abril de 2022**

F: .....

Misael Julio Murudumbay Huerta

C.I: **0350160487**

CERTIFICADO

Certifico que le presente trabajo fue desarrollado por el estudiante: MISAEL JULIO MURUDUMBAY HUERTA, bajo mi supervisión.

Ing. Cristina Flores Urgilés

DIRECTOR DEL TRABAJO DE TITULACIÓN UNIVERSIDAD CATÓLICA DE CUENCA EXTENSIÓN CAÑAR

APROBACIÓN DE TRIBUNAL DE GRADO

El tribunal designado por el honorable consejo directivo de la Universidad Católica de Cuenca Extensión Cañar, Facultad de Ingeniería de Sistemas instalado para receptar la sustentación del trabajo final de investigación con el tema “Marco de Trabajo y Herramientas para el Análisis Forense en la atención de los delitos Informáticos de Cibergrooming bajo los dispositivos móviles Android”, transcurrido el tiempo reglamentario procede a consignar la calificación de (_____/100).

Cañar, _____, de _____, del 202____

_____ _____

PRESIDENTE DIRECTOR

_____ _____

DELEGADO SECRETARIO

DEDICATORIA

A mis padres, Julio Guillermo Murudumbay Fajardo y María Rosa Huerta Montesdeoca, por el apoyo incondicional en esta etapa de formación, a ellos les dedico mi esfuerzo, mi dedicación, mi trabajo.

A mi esposa Jeaneth Carolina Delgado Cazho y a mi hijo Dereck Josué Murudumbay Delgado por ser el pilar fundamental y mi fuerza para salir adelante.

A mis tíos Manuel Huerta y Rosa Guasco, por el apoyo moral y económico, por ser fuente de motivación para alcanzar mis metas.

A mis hermanas Jessica, Karina, Johanna, Sayra Murudumbay Huerta, por sus consejos para seguir adelante con mis estudios y cumplir mis sueños.

AGRADECIMIENTO

Primeramente, agradezco a Dios por permitirme tener tan buena experiencia dentro de la universidad, a los catedráticos de la facultad de Sistemas de manera especial a la Ing. Cristina Flores y al Ing. Cristián Flores por compartir sus conocimientos hacia mi persona en esta etapa de formación y ser el apoyo fundamental en el desarrollo de mi trabajo de titulación.

RESUMEN

La presente investigación tiene por objeto, desarrollar un marco de trabajo con sus respectivas herramientas para el análisis forense, en la atención de los delitos informáticos de cibergrooming, bajo los dispositivos móviles. Los objetivos planteados para el desarrollo de la presente investigación fueron: 1) Analizar documentación científica e identificar aspectos legales en el ecuador a cerca del cibergrooming, 2) Seleccionar la metodología que permita estructurar el proceso de extracción de información de dispositivos móviles, 3) Ejecutar pruebas sobre la herramienta que nos permita recuperar información de los dispositivos móviles utilizando técnicas de informática forense.

La metodología seleccionada fue (DFRW), consta de 4 fases que permiten obtener resultados satisfactorios a la hora de llevar a cabo una investigación forense; en la primera fase de "identificación", se da inicio a la cadena de custodia par el caso de la investigación se tomó como base la prueba electrónica (Teléfono Móvil) para su respectivo análisis, la segunda fase de "recolección", se extrajo contenidos del dispositivo de forma física y lógica (Backup), la tercera fase de "Análisis", se aplicó técnicas y herramienta de análisis forense, utilizando MOBILedit para extracción de información, analizando mensajes, llamadas, fotos, videos, audios, la cuarta fase se realiza la presentación de los hallazgos encontradas en el dispositivo a través de un informe técnico obtenida con la herramienta forense MOBILedit, donde se encontró más de 1000 archivos de imágenes-fotos, con contenido sexual, violencia y burla, consideradas pruebas principales, a ser tomados en cuenta en un juicio.

***Palabras Clave*:** análisis forense, delitos informáticos, cibergroomig, metodología, dfrw.

ABSTRACT

This research work aims at developing a framework with its respective tools for forensic analysis regarding the cybercrime of cyber rooming-in mobile devices. The objectives of the research include: 1) To analyze scientific documentation and identify legal aspects in Ecuador about cyber rooming, 2) To select the methodology to structure the process of extracting information from mobile devices, 3) To run tests on such tool that allows us to recover information from mobile devices using computer forensic techniques. The forensic analysis methodology (DFRW) was the one used, which entails four phases that allow us to obtain satisfactory results when carrying out a forensic investigation.

The first phase embraces "identification", which refers to the chain of custody started for the case of investigation based on electronic evidence (Mobile Phone) for its respective analysis. The second phase refers to "collection", the contents of the device were extracted physically and logically (Backup). The third phase deals with the "Analysis", techniques and forensic analysis tools were applied. The fourth phase is the presentation of the findings encompassed in the device through a technical report obtained with the MOBIL edit forensic tool, where more than 1000 image-photo files were found with sexual content, violence, and mockery, considered as the main evidence to be considered in a trial.

Keywords: forensic analysis, computer crime, cyber rooming, methodology, dfrw.

e-ISSN: 2588-1000

Pro Sciences

Revista de Producción, Ciencias e Investigación

Marco de trabajo y herramientas para el análisis forense en la atención de los delitos informáticos de Cibergrooming bajo los dispositivos móviles Android.

Framework and tools for forensic analysis in the attention of cybergrooming cybercrimes under Android mobile devices.

Misael Julio Murudumbay Huerta[1]
Categoría profesional, Universidad Católica de Cuenca, Ecuador,
mjmurudumbayh87@est.ucacue.edu.ec
ORCID

RESUMEN

La presente investigación tiene por objeto, desarrollar un marco de trabajo con sus respectivas herramientas para el análisis forense, en la atención de los delitos informáticos de cibergrooming, bajo los dispositivos móviles. Los objetivos planteados para el desarrollo de la presente investigación fueron: 1) Analizar documentación científica e identificar aspectos legales en el ecuador a cerca del cibergrooming, 2) Seleccionar la metodología que permita estructurar el proceso de extracción de información de dispositivos móviles, 3) Ejecutar pruebas sobre la herramienta que nos permita recuperar información de los dispositivos móviles utilizando técnicas de informática forense.

La metodología seleccionada fue (DFRW), consta de 4 fases que permiten obtener resultados satisfactorios a la hora de llevar a cabo una investigación forense; en la primera fase de "identificación", se da inicio a la cadena de custodia par el caso de la investigación se tomó como base la prueba electrónica (Teléfono Móvil) para su respectivo análisis, la segunda fase de "recolección", se extrajo contenidos del dispositivo de forma física y lógica (Backup), la tercera fase de "Análisis", se aplicó técnicas y herramienta de análisis forense, utilizando MOBILedit para extracción de información, analizando mensajes, llamadas, fotos, videos, audios, la cuarta fase se realiza la presentación de los hallazgos encontradas en el dispositivo a través de un informe técnico obtenida con la herramienta forense MOBILedit, donde se encontró más de 1000 archivos de imágenes-fotos, con contenido sexual, violencia y burla, consideradas pruebas principales, a ser tomados en cuenta en un juicio.

***Palabras Clave*:** análisis forense, delitos informáticos, cibergroomig, metodología, dfrw.

[1] Ingeniería de Sistema.

INTRODUCCIÓN

El uso de los dispositivos móviles se vuelve cada vez más necesario debido a la gran facilidad para establecer comunicación y manejar información a nivel nacional e internacional, estos dispositivos cuentan con diferentes funciones algunas de ellas son: El acceso a internet, Envió de SMS, E-mails, aplicaciones con conexión a la nube, cámaras, administrador de información personal, Geolocalización, etc.

El uso de estos dispositivos, la información almacenadas en esta y la frecuencia con la que hoy en día se navega en la red, causa un incremento de vulnerabilidades más aun al momento de instalar aplicaciones gratuitas de terceras personas que solicitan información personal para el ingreso al servicio requerido, el uso de las redes sociales es el medio más común para cometer delitos.

Hoy en día las redes sociales son las más utilizados para compartir información entre ellas también están los juegos en línea, siendo una gran ventaja para las personas, pero al mismo tiempo una gran impotencia al momento de cometer una infracción como el: Cibergrooming, que es un delito dirigido principalmente a los niños, se aprovecha de la ingenuidad de los menores de edad, engañándolos con una identidad falsa, para así obtener información confidencial y cometer actos ilícitos.

Realizar un análisis forense requiere de una metodología adecuada, herramientas que permitan obtener de manera rápida la información almacenada en los dispositivos móviles.

Bases Teóricas

El Internet y su beneficio

Internet es una red informática de trasmisión de datos para la comunicación que hace posible el intercambio de todo tipo de información entre sus usuarios, ha sido la herramienta que más rápida acogida ha tenido en la sociedad y también la que más ha cambiado los hábitos y costumbres de las personas (Segovia, 2013).

Internet posee un especial peso en la economía y en la educación. Las TIC han hecho posible: tener fácil acceso a todo tipo de información, disponer de instrumentos para procesar datos de manera rápida, comunicarse con cualquier persona sin importar en que parte del mundo se encuentre mediante el uso de las redes sociales, almacenar gran número de información, interactuar con materiales multimedia, videojuegos, etc. Se está en la realidad de las tecnologías de la información ilimitadas y de la comunicación multidireccional, lo cual conduce a un modelo de sociedad que cuenta con la triple alianza

de la informática, las telecomunicaciones y redes de comunicación, que produce un nuevo modo de interacción personal y una nueva manera de generar y acceder al conocimiento (Segovia, 2013).

La Redes Sociales

"Las redes sociales son herramientas de interacción social, definida como un intercambio dinámico de información entre personas, grupos e instituciones en contexto de complejidad" (Benavides, 2010).

Los usos de las redes sociales han trasformado los estilos de vida y las costumbres de las personas, es decir que la manera en la que estas personas interactúan y se relacionan ha cambiado sustancialmente con la llegada del internet, un sin número de estudiantes usan cada día distintos sitios web de redes sociales, de manera que estas forman parte de su vida cotidiana. Muchos de los estudios que se llevan a cabo hoy en día giran en torno a temas relacionados con la identidad, la privacidad o el uso que los adolescentes hacen de las redes (Segovia, 2013).

Riesgos en el internet y las redes sociales

El internet es una fuente de comunicación moderna, que puede causar adicción social, porque cuando una persona escribe, su único contacto es con la pantalla de un computador o de un teléfono móvil, sin ver ni escuchar a esa persona con la que supuestamente se está comunicando (Benavides, 2010).

El hecho de que las personas expongan con frecuencias sus datos personales en las redes sociales, representa un reto en el tema de privacidad en la red, ya que, quedan expuestas a amenazas que pueden ser aprovechadas por los tratantes y/o explotadores sexuales que detectemos en las redes, timadores, impostores de identidad. El riesgo no se trata solo de ser objeto de observaciones no deseadas de nuestro intercambio epistolar o de nuestros contactos, sino también por la posibilidad de ser víctimas de nuevas formas de delitos y de violencia (Macias, 2018).

El acoso sexual a través de las redes sociales es un problema actual que afecta principalmente a los jóvenes, existen varios métodos de acoso que implica la participación de un adulto contra un menor a través de las redes, entre ellas se mencionan las siguientes:

- *Cibergrooming*

  "Grooming, es una conducta y acciones tomadas por mayores de edad el cual trata de ganar amistad y confianza de niños, niñas y adolescentes con la finalidad de abusar sexualmente de él o ella.". (Mora G. X., 2015)

Cibergrooming, esta conducta se lo hace a través del internet, la utilizan los adultos catalogados como pederastas aprovechándose del anonimato en las redes sociales, foros, chats y así contactar a niños con la finalidad de convencerlos a realizar poses eróticas frente a una cámara, generando material que luego es utilizado como chantaje (Mora G. X., 2015).

Los depredadores ejecutan varias fases para poder cometer el delito.

- Contacto: Mediante identidad Falsa o suplantación de terceros a través de redes sociales.
- Confianza: Por medio de mensajes de texto engañosos.
- Seducción: Manipulación a través de los gustos y preferencias y utiliza el tiempo para fortalecer el vínculo, obteniendo material sexual.
- Amenaza: Extorción, chantaje con publicación de material sexual obtenida del menor.
- Difusión: ejecución del acto de acoso, con la publicación de dicho material obtenido.

- *Sexting*

  Los niños/niñas y adolescentes cometen el error de compartir imágenes de tipo sexual, personal por medios electrónicos. Sin percatarse del peligro de que dicha información sea publicada y visualizada sin su consentimiento (Arab & Diaz, 2015).

- *Ciberacoso*

  Esta agresión también conocida como ciberbullying cosiste en el uso intencionado de las TIC por parte de terceros, con la intención de hostigar, acosar, intimidar, insultar o amenazar a su víctima, se caracteriza al resto por tratarse de una conducta deliberada, realizada a través de medios electrónicos por individuos que, de forma reiterada envían mensajes agresivos a otro individuo con el fin de perjudicar su condición social (Pardo, Herrador, Moya, & Cañigral, 2016).

Delitos Informáticos relacionados al Cibergrooming

Se considera un delito informático, a cualquier incidente donde una víctima se vea afectada o acosada y el criminal del acto cometió el hecho con una computadora, existen un sin número de delitos dentro del código orgánico integral penal, estos delitos son penadas por la ley dependiendo el grado de delito cometido. Para el desarrollo del presente estudio se toman como base los delitos que se encuentran plasmado al cibergrooming.

Código Orgánico Integral Penal del Ecuador

A continuación de describe los delitos referentes al cibergrooming que se encuentran establecidas en los artículos del código orgánico integral penal del Ecuador.

- ***Art. 166:*** *Acoso Sexual.* **–** "La persona que solicite algún acto de naturaleza sexual, para sí o para un tercero, prevaliéndose de autoridad, con la amenaza de causar a la víctima un mal, si la victima sea menor de 18 años de edad serán sancionado con pena de libertad de 3 a 5 años". (Republica del Ecuador Asamblea Nacional, 2021)
- ***Art. 173:*** *Contacto con finalidad sexual con menores de 18 años por medios electrónicos.* – **"**La persona que a través de un medio electrónico proponga concentrar un encuentro con una persona menor, con la finalidad sexual o erótico o la persona que, suplantando la identidad de un tercero o identidad falsa por medios electrónicos, será sancionado con pena privada de 3 a 5 años". (Republica del Ecuador Asamblea Nacional, 2021)
- ***Art. 174:*** *Oferta de servicio sexual con menores de 18 años por medios electrónicos.* – **"**Este articulo sanciona a la persona que, utilice o facilite el correo electrónico, chat, redes sociales, blogs, fotos o cualquier otro medio electrónico para ofrecer servicios sexuales con menores".
- ***Art. 178:*** *Violación a la intimidad.* **-** "Este artículo señala que la persona que, sin contar con la autorización legal, acceda, grabe, reproduzca, difunda o publique datos personales como: mensajes de voz, audio y video que son información contenida en soportes informáticos, comunicaciones privadas de otras personas por cualquier medio, será sancionado con pena privada de la libertad de 1 a 3 años". (Republica del Ecuador Asamblea Nacional, 2021)

Los delitos contra el derecho a la propiedad se encuentran descritos en los siguientes artículos.

- ***Art. 185:*** *Extorción.* – "Este artículo señala que la persona que, con el propósito de obtener provecho personal, obligue a otro, con violencia o intimidación a realizar actos no deseados, será sancionado con pena privada de la libertad de 3 a 5 años". (Republica del Ecuador Asamblea Nacional, 2021)
- ***Art. 212:*** *Suplantación de identidad.* **–** "La persona de cualquier manera suplante la identidad de otra para obtener beneficio para sí, en perjuicio de otra será sancionado con pena privada de libertad de 1 a 3 años". (Republica del Ecuador Asamblea Nacional, 2021)

Procedimiento judicial

"La Constitución ecuatoriana establece que el proceso judicial es una vía para la aplicación de la Justicia; establece los principios de inmediación, oralidad, celeridad, buena fe, lealtad y economía procesal" (Codigo Organico General de Procesos).

En lo que respecta el proceso judicial dentro de la comisión de los delitos informáticos, la participación es de dos o más personas, entre ellas el sujeto activo y el sujeto pasivo; cada uno de ellos realizando acciones diferentes, es decir el primero, es aquel encargado de efectuar todos los actos conducentes para la comisión de la infracción, el segundo, es quien recibe el acto delictivo.

Pruebas

La prueba informática para que sea considerado como tal dentro del proceso penal y surta efectos de validez jurídica debe seguir ciertos parámetros como: ser solicitado, ser presentado, ser practicada, ser incorporada al expediente del proceso penal (Colón Ferruzola Gómez & Cuenca Espinosa, 2014).

- *Evidencia digital*

  Las pruebas digitales encontradas en una escena de un delito pueden servir en un proceso judicial como evidencia probatoria.

  La evidencia digital se puede dividir en tres categorías:

  - ✓ Registros almacenados en un equipo informático: Correos electrónicos, imágenes, documentos ofimáticos, etc.
  - ✓ Registros generados por un equipo informático: Logs de Eventos, logs de errores, logs de transacciones, etc.

- *Mecanismo de prueba*
  - Prueba documental: Físicos, digitales
  - Prueba testimonial: Declaración de terceras personas que conocen respecto a ciertos hechos.
  - Prueba Pericial: Persona experta en determinada área de la ciencia del saber humano, comunica al juez las comprobaciones extraídas de los hechos sometidos a su dictamen.

En caso que la prueba informática requiera pericia alguna, se deberá nombrar un perito informático acreditado por el Consejo Nacional de la Judicatura. Este peritaje debe ser realizado previamente bajo orden judicial para que la prueba obtenida sea válida. E aquí donde actúa la informática forense, con el fin de obtener datos o información de un dispositivo electrónico (Colón Ferruzola Gómez & Cuenca Espinosa, 2014).

Informática Forense

Según Guo et al. (2011), la informática forense se originó a finales de la década de los 80, para referirse al análisis de las computadoras independientes con el objetivo de obtener pruebas digitales.

La informática forense es un proceso que se encarga de la identificación, extracción e interpretación de las evidencias encontradas en los dispositivos electrónicos.

- *Peritaje informático forense*

  El peritaje informático forense se encarga del proceso de identificación, adquisición, preservación, análisis y presentación de evidencias digitales, de acuerdo a procedimientos técnicos y legales preestablecidos, como apoyo a la administración de justicia en la resolución de un caso Legal (Esteben & Esteban, 2009).

Análisis forense en dispositivos móviles

Actualmente existen gran variedad de dispositivos móviles dentro de los cuales el mayor crecimiento en popularidad y utilidad se presentan los teléfonos inteligentes ya que estos poseen una capacidad para realizar llamadas desde aplicaciones de mensajería y videos conferencias solamente utilizando la conexión a internet, además, estos dispositivos permiten que los usuarios puedan navegar por internet emulando ser ordenadores que cumplen con la misma función. Finalmente, estos proporcionan un desarrollo y ejecución de aplicaciones que no son incluidas por el fabricante (David, 2020).

El análisis forense sobre dispositivos móviles es un campo relativamente nuevo debido a que sus procedimientos y normas se encuentran desarrollándose por la cual se ha verificado la carencia de herramientas forenses para Linux y Windows hoy en día (David, 2020).

Herramienta utilizada en la informática forense

Para determinar el estado de un sistema después de que sus medidas de seguridad han sido vulneradas, es decir, después de que se intentó o se cometió un delito informático, la informática forense utiliza las

herramientas necesarias (según el caso que se esté investigando) para buscar y analizar evidencia que permitan identificar los mecanismos o técnicas que se utilizaron para acceder al sistema de una forma inadecuada (Luisa Fernanda Castillo Saavedra, 2015).

Metodologías de Informática Forense

La informática forense consiste en la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal en la detección de algunas instrucciones (Cajo, Pucuna, Cajo, Coronado, & Orozco, 2018).

Estudios Previos

Existen estudios realizados por muchas personas acerca de la herramienta y metodologías utilizadas para análisis forense en la atención de delitos informáticos.

En un estudio similar realizado por Estrada, A. C. (2010) y publicado en Colombia por la Revista Pensamiento Americano, que lleva por título "La Informática Forense y los Delitos Informáticos" se centra en la importancia de la informática forense, las metodologías que son utilizadas y las herramientas tecnológicas que permiten llevar acabo el análisis forense de los delitos informáticos, este articulo menciona dos herramientas para extracción de datos forense, estas son: Encase, Forensic toolkit siendo las herramientas reconocidas a nivel mundial, con un costo de 4.000 o 5.000$.

Otra investigación similar Realizada por Cajamarca, B. (2017) titulada como "Marco de trabajo estandarizado para el análisis forense de la evidencia digital" estudio realizado con la finalidad de constituir un marco de trabajo para llevar a cabo un correcto análisis forense, en cuanto a las evidencias electrónicas generadas por causa de delitos informáticos.

En base a estas investigaciones se determina que Byron Cajamarca autor del artículo elaboro un marco de trabajo propio para el análisis forense, para ello utiliza la metodología UNE 71506:2013, debido a que es la más completa para el manejo de evidencias digitales y es de gran ayuda para los peritos Informáticos a la hora de realizar una investigación forense.

Hidalgo Cajo, I. (2018) realiza un "Estudio comparativo de las metodologías de análisis forense informático para la examinación de datos en medios digitales" el objetivo de esta investigación tiene como propósito la obtención de una metodología recomendable para un correcto análisis forense informático, a base de una comparación entre las diferentes metodologías de análisis forense que existan.

El autor Hidalgo Cajo, concluye su investigación con el desarrollo de una metodología estandarizada, en el cual menciona que dicha metodología facilita las tareas de análisis, estudio y adquisición de los elementos de un peritaje informático, realiza un estudio comparativo con diferentes normar en la cual la mayoría de los investigadores optan por utilizar la norma UNE 71506:2013.

Existe otra investigación desarrollada en la ciudad de cuenca, el estudio fue realizado por Quizhpe, G. (2015) trabajo que lleva por título "Metodología de la Informática Forense en la Atención de Delitos Informáticos de Cibergrooming" orientada a la implementación de la metodología de informática forense para encontrar las evidencias claras de los delitos cometidos por las personas que suplantan la identidad de otra para llegar a los jóvenes y perjudicarlos.

La presente investigación utiliza la herramienta Lads para búsqueda de archivos ocultos, una metodología propia y para su respectivo análisis fue montado sobre la aplicación VMWare Workstation en el cual se utilizó la herramienta forense misionada anteriormente.

METODOLOGÍA

El presente estudio se lleva a cabo mediante la aplicación de la metodología Digital Forensics Research Workshop (DFRW), la cual consta de 4 fases para el análisis que son: Identificación, Recolección, Análisis y Presentación, cada una de ellas cumpliendo un proceso específico. El método utilizado para el desarrollo de la investigación es inductivo, debido a que se realiza una investigación sobre los conceptos fundamentales, la misma que se lleva a cabo mediante una revisión a diferentes fuentes como: libros, artículos científicos y tesis, con el fin de profundizar enfoques relacionados al tema de investigación y experimental por las pruebas realizadas con el software seleccionado MOBILedit Forensic, herramienta que permite la recuperación de información relevante para el análisis del caso. La metodología planteada como estrategia para el desarrollo del presente marco de trabajo fue seleccionada a partir de varias investigaciones sobre el tema "Análisis forense en dispositivos móviles Android" realizada por diferentes autores como: (Quizhpe Mora, 2015); (Cuenca Alvarado, 2015); (Guaman Guanopatin, 2014), en las cuales elaboran comparaciones entre distintos métodos para el análisis forense, en base a ello se determinaron las fases de análisis y algunos criterios particulares para su respectiva valoración, comprobando así cuales cumplen y cuáles no, obteniendo como resultado una matriz de peso tal como se visualiza en la Tabla 1.

Matriz de calificación para los criterios establecidos

La valoración de las metodologías con el enfoque a cada criterio se llevará a cabo mediante la calificación 0 a 1, donde le numero 0 será una respuesta negativa (No cumple) y el numero 1 será una respuesta positiva (Cumple), dichos valores fueros propuestos en base a una investigación detallada en la Tabla 1.

Tabla 1: Para la obtención de la matriz se le otorga un peso a cada fase de análisis forense, en este caso el valor agregado para su respectiva sumatoria es el número 1, las mismas que serán cuantificadas en base al cumplimiento de cada metodología. El peso fue determinado en base a una matriz realizada por Diego Pinto (2014), en su artículo titulado "Metodologías de análisis forense orientado a incidentes en dispositivos móviles".

Criterios de valoración Fase de análisis forense	Metodologías de análisis forense informático				
	ISO 27037:2012	Metodología Del Departamento de Justicia(DOJ)	Metodología del Instituto SANS	Digital Forensics Research Workshop (DFRW)	Kevin Mandia y Chris Prosise
Identificación	1	1	1	1	1
Recolección	1	1	1	1	1
Análisis	1	1	1	1	1
Presentación			1	1	1
Total	3	3	4	4	4

Criterios de valoración	**Metodologías de análisis forense informático**				
	ISO 27037:2012	Metodología del Departamento de Justicia(DOJ)	Metodología del Instituto SANS	Digital Forensics Research Workshop (DFRW)	Kevin Mandia y Chris Prosise
Cubre con todos los pasos generales para realizar una investigación de cómputo forense.	-	0	1	1	1
Implementación en todos los dispositivos.	1	0	0	1	0
Manejo de grandes volúmenes de Información información.	1	0	0	1	0
Respuesta a las técnicas para ocultar datos.	-	0	1	1	1
Total	2	0	2	8	2

Suma Total	5	3	6	8	6

Nota: Según el peso otorgado (1), en la primera comparación de las fases se obtiene los resultados para cada metodología analizada, de la misma manera se hace uso del mismo peso para realizar la siguiente comparación con los criterios establecidos, con la sumatoria de ambos resultados, se obtiene un total para cada metodología, a partir de ello se realiza la respectiva selección.

La metodología con mayor puntuación fue Digital Forensics Research Workshop (DFRW), siendo la metodología utilizada para la ejecución de análisis forense en los dispositivos móviles Android, puesto que cubre con todas las fases requeridas para hacer una investigación forense y cumple con cada uno de los criterios expuestos, además de ello DFRW está enfocado a conservar la integridad y mantener la cadena de custodia.

RESULTADOS

Una vez obtenido la herramienta y la metodología, se procede a realizar las pruebas en dos dispositivos móviles, facilitados para el examen forense. A continuación, se describe cada una de las fases de la metodología.

Fase1: Identificación

En esta fase se realiza un análisis del entorno, tanto técnico como formal del procedimiento, para obtener la evidencia digital, para ello se debe considerar diferentes aspectos como: El tipo de delito, el lugar en el que se encuentra, cuál es la evidencia informática y el proceso a aplicar.

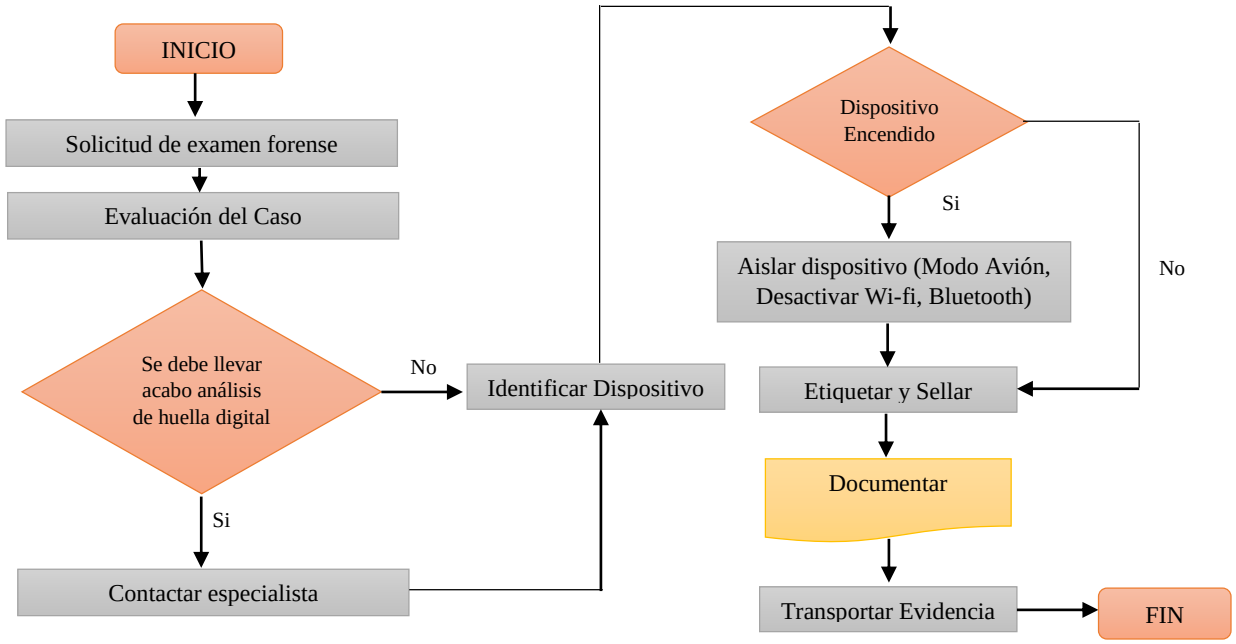


Ilustración 1: Fase de Identificación; Autor: Propio.

Evaluación de caso de estudio

Se procede con la recepción de la solicitud emitida por la fiscalía, para dar inicio al proceso de análisis forense.

Al ser un caso de estudio de prueba, se aclara que el componente a ser analizado son dos dispositivos móviles (Samsung Galaxy J8, Huawei Y9 2019), con el único fin de localizar información que corrobore con el proceso de investigación del Cibergrooming, para ello se sigue un proceso específico para la preservación de la evidencia, así como la incautación de los dispositivos para el análisis respectivo.

Una vez en el lugar de los hechos, los dispositivos son colocados en una envoltura y sellado, posterior a ello se le coloca en una bolsa antiestética para ser trasladado como evidencia.

Descripción de la evidencia

Evidencia

Código	Cantidad	Dispositivo	Estado	descripción
MA001	1	Smartphone	Encendido	Sistema Operativo: Android Marca: Samsung Modelo: SM-J810M Almacenamiento: 23.6 GB Tarjeta Externa: 7.2 GB Color: Plateado Conectividad a internet: Wifi Puerto: USB
MA002	2	Smartphone	Encendido	Sistema Operativo: Android Marca: Huawei Y9 2019 Almacenamiento: 23.6 GB Tarjeta Externa: 7.2 GB Color: Negro Conectividad a internet: Wifi Puerto: USB

Fase 2: Recolección – Adquisición

Una vez que la evidencia este en el poder del perito, se procede a recolectar los datos del dispositivo tanto físico (Datos de la unidad física) como lógico (Archivos), para ello se procede a calcular el hash del dispositivo y obtener la imagen de los mismos, utilizando la herramienta FTK Imager, teniendo instalada dicha herramienta se procede a conectar el dispositivo al equipo mediante el cable de datos USB.

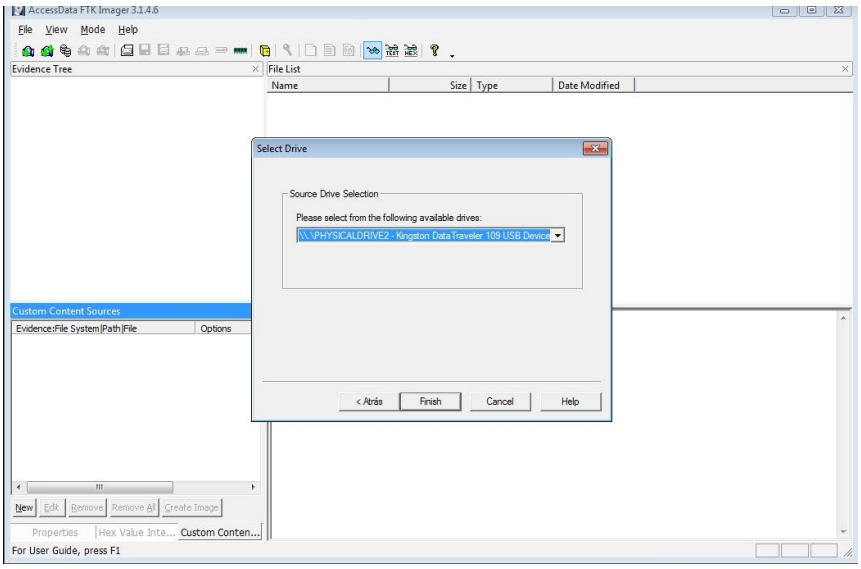


Ilustración 2: Proceso para la obtención de la imagen del teléfono; autor: Propio.

Con el proceso realizado en la herramienta, se pudo calcular el hash la misma que garantiza la autenticidad de los archivos y obtener las imágenes de los dispositivos involucrados, de la cual se realizó el análisis forense que se describe a continuación.

Tabla 2: Obtención del Hash, Dispositivo A.

Dispositivo A	
Nombre de la Imagen	Samsung SM-J810M (R58M14XT73P)
Hash	cd9988fc0669e0b1aab06e2f3d2fac03f9032e54ebdb73103da1a6f50bd373bb

Tabla 3: Obtención del Hash, Dispositivo B

Dispositivo B	
Nombre de la Imagen	Huawei Y9 2019
Hash	d2251dcf7d68c766e1953c786f9a2f36

Luego de haber obtenido la imagen, se procede con el análisis de la herramienta MOBILedit, el cual proporciona los siguientes datos: información del dispositivo, cuentas eliminadas, contactos, mensajes, llamadas, calendarios, videos, aplicaciones, archivos multimedia, Audio, etc.

Posterior a lo indicado se realiza un registro de la cadena de custodia, el cual consta de un formulario donde se registra toda la información básica, evitando que se rompa la cadena de custodia.

Fase 3: Análisis y explotación

En esta fase se lleva a cabo el proceso técnico, es decir que mediante el uso de la herramienta (MOBILedit), se realiza un análisis más profundo con el fin de encontrar pruebas contundentes en la investigación.

Procedimiento

Como ya se mencionó en el punto anterior la herramienta seleccionada facilita una variedad de opciones, para el caso de la investigación de procederá a obtener los siguientes: mensajes, llamadas, imágenes-Fotos, siendo pruebas contundentes en el caso del Cibergrooming, a la cual se enfoca el presente estudio.

Para la extracción de datos se utiliza la imagen del dispositivo obtenida en la fase anterior y con la ayuda de MOBILedit extraemos los archivos de interés.

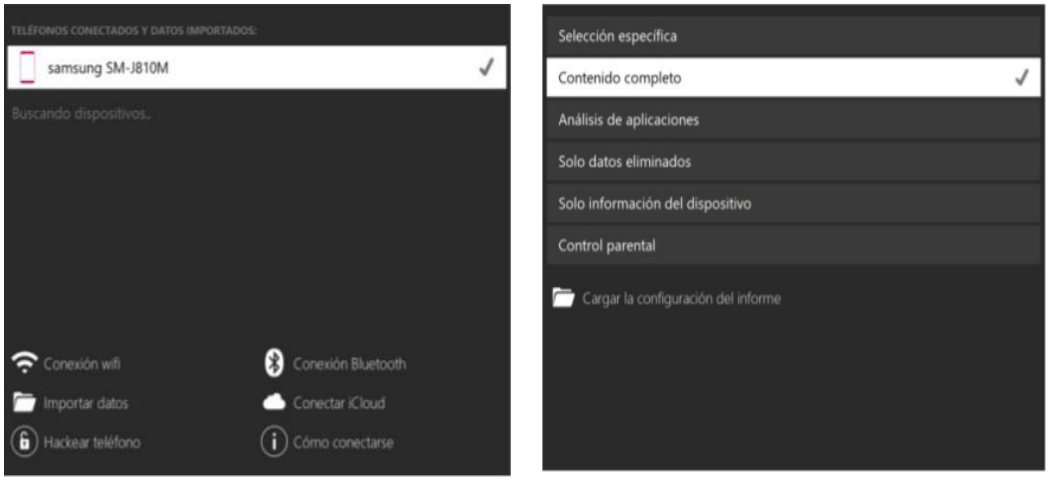


Ilustración 3: Proceso de extracción de datos; Autor: Propio.

Resultados

Al finalizar el proceso de extracción de la imagen, la información recuperada de los dispositivos móviles, se detallan a continuación tanto del dispositivo A como del dispositivo B.

Mensajes – Dispositivo A

De acuerdo al análisis en el dispositivo A, se obtuvo como resultado un total de 107 mensajes realizados, de las cuales mantuvo conversaciones con 10 contactos registrados y 1 no registrado, cabe recalcar que este dispositivo ha recibido con frecuencia SMS de un número desconocido en

fechas recientes. A continuación, se presenta el resultado obtenido con la ejecución de la herramienta, Ilustración Nª 4.

Ilustración 4: Mensajes recibidos del dispositivo B; Autor: Herramienta MOBILedit.

Mensajes – Dispositivo B

De acuerdo al análisis en el dispositivo B, se obtuvo como resultado un total de 40 mensajes realizados, de las cuales mantuvo 7 conversaciones, la herramienta permite obtener los SMS de forma detallada, gracias a ello se pudo evidenciar que esta persona envió con frecuencia SMS a unos de sus contactos. A continuación, se presenta los SMS enviados a su contacto, Ilustración Nª 5.

Ilustración 5: Mensajes enviados del dispositivo B al Dispositivo A; Autor: Herramienta MOBILedit.

Llamadas - Dispositivo A

Se obtuvo un total de 326 registros de llamadas, las mismas que se realizaron en el presente año, entre estas se encontraron llamadas recibidas del mismo número telefónico que recibe los SMS. La información obtenida se visualiza de la siguiente manera, Ilustración Nª 6.

Leyenda:

Llamada marcada | Llamada recibida | Llamada perdida | Llamada rechazada | Mensaje de voz

	Etiqueta	Desde / A	Hora	Duración
1	David	Desde: David, 0984883019	2021-12-18 10:04:53 (UTC-5)	00:00:15
2	ing Cis	Desde: ing Cis, 0998156996	2021-12-18 10:08:51 (UTC-5)	00:00:44
3	David	Desde: David, 0984883019	2021-12-18 12:02:31 (UTC-5)	00:00:12
4	David	Desde: David, 0984883019	2021-12-18 12:02:56 (UTC-5)	00:00:13
312		Desde: 0987746946	2022-03-31 11:15:07 (UTC-5)	00:00:00
313		Desde: 0987746946	2022-03-31 11:15:27 (UTC-5)	00:00:12
314		Desde: 0987746946	2022-03-31 11:20:53 (UTC-5)	00:00:00
315		Desde: 0987746946	2022-03-31 11:21:19 (UTC-5)	00:00:23

Ilustración 6: Registros de llamadas recibidas- Numero del dispositivo B; Autor: Herramienta MOBILedit.

Llamadas - Dispositivo B

Se obtuvo un total de 69 registros de llamadas, las mismas que se realizaron en el presente año, entre estas se encontraron llamadas marcadas al mismo número telefónico a la que envía los SMS. La información obtenida se visualiza de la siguiente manera.

Leyenda:

Llamada marcada | Llamada recibida | Llamada perdida | Llamada rechazada | Mensaje de voz

	Etiqueta	Desde / A	Hora	Duración
1	Mi Reina❤	A: Mi Reina❤, 0999250969 (Mi Reina❤)*	2022-01-12 10:27:32 (UTC-5)	00:00:00
2		A: 0984696998	2022-01-12 10:33:05 (UTC-5)	00:00:00
3		Desde: 0984696998	2022-01-12 10:34:44 (UTC-5)	00:00:39
4		Desde: 0984696998	2022-01-12 10:56:49 (UTC-5)	00:00:31
5		A: 0998070504	2022-01-12 11:20:44 (UTC-5)	00:00:00
6		A: 0998070504	2022-01-12 11:56:04 (UTC-5)	00:01:18
63	Jose Iglesias	A: Jose Iglesias, +593992619090	2022-03-31 11:09:51 (UTC-5)	00:00:00
64	Jose Iglesias	A: Jose Iglesias, +593992619090	2022-03-31 11:10:07 (UTC-5)	00:00:00

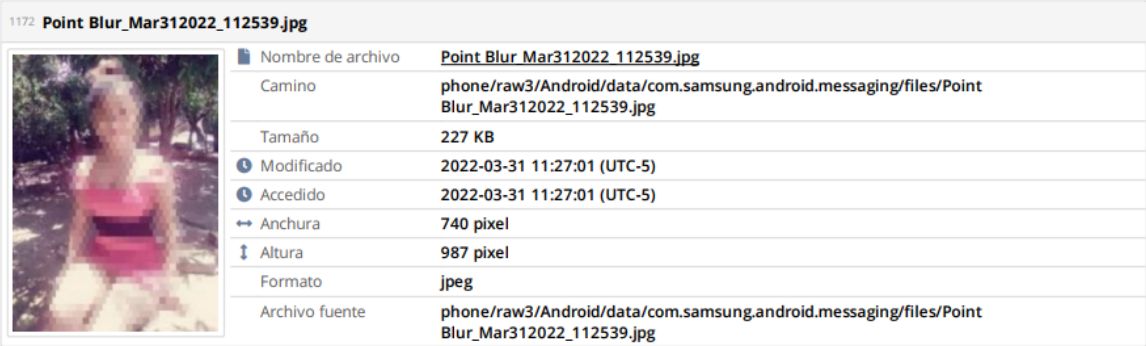
Ilustración 7: Llamadas marcadas- Número telefónico dispositivo A; Autor: Herramienta MOBILedit.

Imágenes - Dispositivo A

Se obtiene un total de 500 imágenes y fotos, de las cuales 300 son realizadas mediante la aplicación B612 y la aplicación propia del dispositivo, 100 descargas y 100 imágenes considerados captura de pantalla.

Imágenes - Dispositivo B

Se obtiene un total de 1230 imágenes y fotos, de las cuales 660 son realizadas por diferentes aplicaciones de cámara del dispositivo y 570 son descargas realizadas. La mayoría de las imágenes son similares a la que se presenta en la siguiente Ilustración Nª.



DISCUSIÓN

En el ecuador al igual que en otros países existen normativas que regulan las conductas comisivas que se presenta día a día con el avance de los medios tecnológicos, dichas normas o leyes facilitan a los jueces a impartir justicia según sea el caso requerido.

En cuanto a la cuestión legal interna en el ecuador, se menciona la resolución de la corte nacional de justicia Nº 3-15 del suplemento 462 de 19 de marzo del 2015, en el cual disponen: "No cabe recurso de casación contra las sentencias dictadas por contravenciones de violencia a la mujer o miembros del núcleo familiar, ni cometidos por adolescentes", es decir, existen nuevas conductas delictivas relacionadas con el Cibergrooming, de las cuales se encuentran tipificadas desde el Art. 166 al Art. 212 de la sección 4, 5, 6, 7, 8, 9 "Delitos" del código orgánico integral penal, las mismas que son sancionadas con pena privada de la libertad de 5 a 10 años según la gravedad del caso.

El proceso judicial involucra una serie de pasos, como la recolección de evidencias que constituye el inicio de la cadena de custodia, luego se procede al embalaje, que hace referencia a la protección de la evidencia y así mismo al etiquetado que corresponde a colocar toda la información del caso.

Para llevar a cabo el proceso pericial se ha utilizado una metodología específica, cumpliendo con los principios fundamentales de la informática forense, se utilizó la herramienta de software forense especializado, que permitió obtener cada una de las pruebas especificadas.

El análisis fue realizado en dos dispositivos móviles facilitados para la ejecución del examen forense, siendo esta un teléfono Samsung Galaxy J8 y un Huawei Y9 2019, de las cuales se logró extraer todos los archivos necesarios.

Para la extracción de datos, se ejecutó la herramienta seleccionada MOBILedit, con la cual se pudo obtener diferentes tipos de información de los dispositivos móviles, con respecto al caso investigativo enfocado al delito informático cibergrooming, se seleccionó los datos más importantes a ser recuperados, mencionando que las pruebas más importantes para dicho delito son: registros de llamadas, registros de mensajes, fotos, etc., las mismas que un juez solicita la recuperación dicha información.

De acuerdo a la información obtenida, se consiguieron pruebas que pueden ser tomadas en cuenta para la decisión de un juez sobre un caso del cibergrooming, estas fueron llamadas y mensajes constantes realizadas hacia el dispositivo (A), obteniendo como resultados un total de 326 llamadas, de las cuales 15 de ellas son llamadas recibidas y 30 llamadas perdidas, que corresponde al número celular del dispositivo (B) analizado. Por otra parte, se obtuvo un total de 106 SMS entre estas se encontraron mensajes exigentes y amenazadoras enviadas desde el dispositivo B, cabe mencionar también que en el dispositivo móvil B se encontraron fotos, imágenes intimas de terceras personas y estas coinciden con lo encontrado en el dispositivo (A), entre los hallazgos se determinó también que algunas de las fotos y sms fueron archivos eliminados las misma que gracias a la herramienta pudieron ser recuperadas.

CONCLUSIONES

Con la metodología propuesta para el desarrollo del presente estudio fue posible identificar el proceso a seguir, al momento de realizar una investigación forense, teniendo como evidencia un dispositivo Móvil Android, lo cual permite analizar, obtener y manejar adecuadamente la evidencia digital.

La herramienta seleccionada permitió tener una mejor perspectiva de la información encontrada, pero cabe recalcar que, el análisis de la información muchas veces se ve afectada por los diferentes modelos de los dispositivos y de las aplicaciones instaladas.

Una de las funciones de un investigador forense, es la de controlar los delitos que se presenta en las redes sociales, siendo el medio donde más se llevan a cabo estos actos ilícitos, protegiendo así a niños/as y adolescentes vulnerables, así como también encontrar a los culpables para sancionarlos según lo especifique el en código orgánico integral penal.

Cuando se comete un delito y existe la denuncia de la mismas, esta debe seguir un debido proceso en presencia de un fiscal y el perito forense, ya que su deber es obtener toda la información de lo sucedido, materializar todas las pruebas encontradas para demostrar así la inocencia o culpabilidad del acusado, dichas pruebas deben ser válidas para la disputa en un juicio.

El código orgánico integral penal en su Art. 191 "Modificación de información de equipos terminales móviles" dicta que toda persona que modifique la información de los equipos, serán sancionados con pena privada de libertad de 1 a 3 años.

REFERENCIAS BIBLIOGRÁFICAS

Afrodita, G. G. (01 de 10 de 2017). *repositorio.uta.edu.ec.* Recuperado el 25 de 08 de 2021, de https://repositorio.uta.edu.ec/bitstream/123456789/26929/1/Tesis_t1336si.pdf

Afrodita, G. G. (01 de 10 de 2017). *repositorio.uta.edu.ec.* Recuperado el 25 de 10 de 2021, de https://repositorio.uta.edu.ec/handle/123456789/26929

Arab, E., & Diaz, A. (01 de 01 de 2015). *reader.elsevier.com.* Recuperado el 22 de 10 de 2021, de https://reader.elsevier.com/reader/sd/pii/S0716864015000048?token=343CCB87199B5932907FF9987EB7C0CA8E70C04DC44299A0164C327CA3D894A897096A51A54796F333342EA8956D2F14&originRegion=us-east-1&originCreation=20211022170242

AREITIO BERTOLIN, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* España: Editorial Paraninfo.

Benavides, P. A. (01 de 06 de 2010). *dspace.ups.edu.ec.* Obtenido de dspace.ups.edu.ec: https://dspace.ups.edu.ec/bitstream/123456789/2618/1/Tesis%20Impacto%20de%20las%20Redes%20Sociales%20y%20el%20Internet.pdf

Blanco, P. J. (11 de 03 de 2014). *eunir.unir.net.* Recuperado el 23 de 06 de 2021, de https://reunir.unir.net/bitstream/handle/123456789/2828/arnedo%20blanco.pdf?sequence=1&isAllowed=y

Blanco, P. J. (03 de 11 de 2014). *reunir.unir.net.* Recuperado el 25 de 05 de 2021, de https://reunir.unir.net/bitstream/handle/123456789/2828/arnedo%20blanco.pdf?sequence=1&isAllowed=y

Cajamarca, B. G., & Sebastián, G. L. (01 de 01 de 2017). *repositorio.uisek.edu.ec.* Recuperado el 26 de 05 de 2021, de https://repositorio.uisek.edu.ec/bitstream/123456789/2991/1/71.%201390-9304%20GRIJALVA%20JUAN%202017.pdf

Cajo, I. M., Pucuna, S. Y., Cajo, B. G., Coronado, V. M., & Orozco, F. V. (01 de 06 de 2018). *eujournal.org.* Recuperado el 26 de 05 de 2021, de https://eujournal.org/index.php/esj/article/view/10956

CARRIZO, S. A. (01 de 01 de 2017). *repositorio.uesiglo21.edu.ar.* Recuperado el 25 de 05 de 2021, de https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/14054/CARRIZO%20SILVINA%20ANDREA.pdf?sequence=1&isAllowed=y

Codigo Organico General de Procesos . (s.f.). *funcionjudicial.gob.ec.* Obtenido de funcionjudicial.gob.ec: https://www.funcionjudicial.gob.ec/pdf/Codigo%20Organico%20General%20de%20Procesos.pdf

Colón Ferruzola Gómez, E., & Cuenca Espinosa, H. A. (2014). Cómo responder a un Delito Informático. *Revista Ciencia Unemi*, 1-9.

Cuenca Alvarado, J. K. (31 de 03 de 2015). *dspace.utpl.edu.ec.* Obtenido de dspace.utpl.edu.ec: http://dspace.utpl.edu.ec/jspui/handle/123456789/11815

David, K. S. (01 de 01 de 2020). *http://repositorio.ug.edu.ec/.* Recuperado el 15 de 06 de 2021, de http://repositorio.ug.edu.ec/bitstream/redug/48800/1/B-CINT-PTG-N.497%20Aguirre%20David%20Katty%20Stefania.pdf

Esteben, C. V., & Esteban, P. D. (01 de 01 de 2009). *dspace.uazuay.edu.ec.* Recuperado el 27 de 06 de 2021, de http://dspace.uazuay.edu.ec/bitstream/datos/2398/1/07435.pdf

Estrada, A. C. (2010). La informática forensey los delitos informáticos. *Revista Pensamiento Americano*, 81-88.

Flores, C., Flores, C., Guasco, T., & Leon-Acurio, J. (2019). A Diagnosis of Threat Vulnerability and Risk as It Relates to the Use of Social Media Sites When Utilized by Adolescent Students Enrolled at the Urban Center of Canton Cañar. *Communication in Commputer annd Information Science*, 200-214.

Graciela Viaña, L. F. (01 de 01 de 2017). *http://sedici.unlp.edu.ar/.* Recuperado el 10 de 06 de 2021, de http://sedici.unlp.edu.ar/bitstream/handle/10915/104062/Documento_completo.pdf-PDFA.pdf?sequence=1

Guaman Guanopatin, E. P. (01 de 05 de 2014). *repositorio.espe.edu.ec/.* Recuperado el 24 de 08 de 2021, de http://repositorio.espe.edu.ec/bitstream/21000/9646/5/T-ESPE-048287.pdf

Guzman, J. A., & Forrero, L. A. (01 de 01 de 2013). *epository.unipiloto.edu.co.* Recuperado el 15 de 06 de 2021, de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2691/00001524.pdf?sequence=1

Hernández, C. A. (01 de 01 de 2018). *http://artemisa.unicauca.edu.co/.* Recuperado el 14 de 06 de 2021, de http://artemisa.unicauca.edu.co/~rhernandez/articulos/Articulo_UPM-Criptored_Symbian_OS_Forensics_UJaveriana.pdf

Hong Guo, B. J. (2011). *Research and Review on Computer Forensics.* China: e-Forensics 2010.

ISOTools Excellence. (26 de 01 de 2017). *pmg-ssi.com*. Recuperado el 23 de 06 de 2021, de https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Luisa Fernanda Castillo Saavedra, J. A. (01 de 01 de 2015). Informática Forense en Colombia. *Ciencia, Innovacion y tecnologia, 2*, 1-12. Recuperado el 28 de 06 de 2021, de https://www.jdc.edu.co/revistas/index.php/rciyt/article/view/113

Macias, M. J. (01 de 08 de 2018). *repositorio.uleam.edu.ec.* Obtenido de repositorio.uleam.edu.ec: https://repositorio.uleam.edu.ec/bitstream/123456789/1756/1/ULEAM-PER-0031.pdf

Magaly, Q. M. (01 de 01 de 2018). *dspace.uce.edu.ec.* Recuperado el 03 de 06 de 2021, de http://www.dspace.uce.edu.ec/bitstream/25000/17149/1/T-UCE-0013-JUR-129.pdf

Mora, G. X. (01 de 02 de 2015). *dspace.ups.edu.ec.* Recuperado el 26 de 05 de 2021, de https://dspace.ups.edu.ec/handle/123456789/7784

Mora, G. X. (01 de 02 de 2015). *dspace.ups.edu.ec.* Recuperado el 22 de 10 de 2021, de https://dspace.ups.edu.ec/handle/123456789/7784

Pardo, L. S., Herrador, G. C., Moya, R. A., & Cañigral, F.-J. B. (01 de 01 de 2016). *fundacioncsz.org.* Obtenido de fundacioncsz.org: http://www.fundacioncsz.org/ArchivosPublicaciones/292.pdf

Pinto, D. (17 de 10 de 2014). *publicaciones.ucuenca.edu.ec.* Recuperado el 26 de 05 de 2021, de https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/view/721/641

Quizhpe Mora, G. X. (01 de 02 de 2015). *dspace.ups.edu.ec.* Obtenido de dspace.ups.edu.ec: http://dspace.ups.edu.ec/handle/123456789/7784

Republica del Ecuador Asamblea Nacional. (17 de 02 de 2021). *defensa.gob.ec.* Recuperado el 22 de 10 de 2021, de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

RONQUILLO, J. S. (01 de 01 de 2016). *repositorio.ug.edu.ec.* Recuperado el 03 de 06 de 2021, de http://repositorio.ug.edu.ec/bitstream/redug/18108/1/UG-FCMF-B-CINT-PTG-N.104.pdf

Sampaoli, J. A. (06 de 12 de 2018). *repositorio.uca.edu.ar.* Recuperado el 28 de 06 de 2021, de https://repositorio.uca.edu.ar/bitstream/123456789/523/11/peritaje-marco-tecnico-practico.pdf

Segovia, M. I. (01 de 05 de 2013). *rua.ua.es.* Obtenido de rua.ua.es: https://rua.ua.es/dspace/bitstream/10045/35701/1/Tesis_Laguna_Segovia.pdf

Solarte Solarte, F. N., Enriquez Rosero, E. R., & Benavides Ruano, M. d. (01 de 12 de 2015). *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informatica y de información bajo la norma ISO/IEC 27001*. Recuperado el 22 de 06 de 2021, de https://pdfs.semanticscholar.org/2112/fc98704ec5bb6121443caaa6ebd6583f6c2e.pdf

TAPIA, P. N., & GALLARDO, M. F. (01 de 11 de 2009). *repositorio.utc.edu.ec.* Recuperado el 23 de 06 de 2021, de http://repositorio.utc.edu.ec/bitstream/27000/139/1/T-UTC-0066.pdf

ANEXOS: Protocolo de investigación

Trabajo de Titulación

Tema:

Marco de trabajo y herramientas para el análisis forense en la atención de los delitos informáticos de Cibergrooming bajo los dispositivos móviles.

Unidad Académica

Tecnologías de la Información y la Comunicación

Carrera

Ingeniera de Sistemas

Alumno

Misael Julio Murudumbay Huerta

Tutor:

Ing. Cristina Flores

Abril – Agosto-2021

Cañar, 22 de abril de 2021

Ingeniero
Leopoldo Pauta Ayabaca, Msc.
DECANO DE LA UNIDAD ACADÉMICA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Ciudad.

Yo, **MISAEL JULIO MURUDUMBAY HUERTA**, con número de identificación **0350160487,** alumno de la carrera de Ingeniería de Sistemas, solicito por su intermedio a Consejo Directivo la aprobación del tema de tesis **"MARCO DE TRABAJO Y HERRAMIENTAS PARA EL ANÁLISIS FORENSE EN LA ATENCIÓN DE LOS DELITOS INFORMÁTICOS DE CIBERGROOMING BAJO LOS DISPOSITIVOS MÓVILES.", ** proponiendo como tutor de la misma a la Ing. Cristina Flores Urgiles, el tema propuesto está considerado su desarrollo en décimo ciclo, ya que estaré matriculada en la Unidad de Titulación.

Por la atención que Ud. y el Honorable Consejo Directivo le brinden a la presente, anticipo mis sentimientos de consideración y estima para cada uno de Uds.

Atentamente;

Sr. MISAEL JULIO MURUDUMBAY HUERTA
Estudiante de Ingeniería de Sistemas, extensión Cañar
CI: 0350160487

A. TÍTULO

Marco de trabajo y herramientas para el análisis forense en la atención de los delitos informáticos de Cibergrooming bajo los dispositivos móviles.

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Energía eléctrica y tecnologías de la información para la innovación y el desarrollo sostenible.	**Ciencia de los ordenadores, Analítica de datos y algoritmos computacionales.**	Analítica de Datos	
		Ingeniería de Software	
		Algoritmos Computacionales	
		Inteligencia de Negocios	
		Gobierno de TI	
		Auditoria y seguridad informática	x
		Simulación	

C. PLANTEAMIENTO DEL PROBLEMA

En estos últimos tiempos el uso de las herramientas tecnológicas ha ocasionado problemas de delitos informáticos como es el caso del cibergrooming que surgen por personas mayores de edad con el objetivo de someter a una persona menor de edad al acoso sexual, es por ello que las personas menores de edad no son conscientes del peligro que surgen a través de las redes sociales, el internet por implicaciones que van sometidas sin seguridad, considerando actitudes intimidatorias, agresivas , mal intencionadas y repetidas que tiene como finalidad de hacer el mal al prójimo con el control sobre un menor de edad ocasionando chantaje, humillaciones y amenazas, la informática forense brinda pautas importantes para prevenir, actuar y aplicar la ley frente a casos de cibergrooming, determinando lo sucedido considerando los sucesos más importantes para comprobar que el delito informático sea real, tomando como base las evidencias de los equipos que guardan la información digital.

Es por ello que se debe analizar las herramientas forenses para identificar el tipo de delito cometido en el que una persona menor de edad es víctima determinando a través de los equipos informáticos que guardan la

información digital a través de los peritos informáticos que analizan la información del caso que suceda, de los dispositivos móviles siendo una herramienta de mayor utilidad, factibilidad en el día a día de la vida de las personas en diferentes actividades cotidianas.

D. OBJETIVO GENERAL

Desarrollar un marco de trabajo con sus respectivas herramientas para el análisis forense en la atención de los delitos informáticos de cibergrooming bajo los dispositivos móviles.

E. OBJETIVOS ESPECÍFICOS

1. Analizar documentación científica e Identificar aspectos legales en el Ecuador a cerca del Cibergrooming.
2. Seleccionar la metodología que permita estructurar el proceso de extracción de información de dispositivos móviles sobre la base del delito de Cibergrooming.
3. Ejecutar pruebas sobre las herramientas que nos permita recuperar información en los dispositivos móviles utilizando técnicas de informática forense.

F. JUSTIFICACIÓN

El avance de la tecnología cada vez va evolucionando más en este caso el internet, herramienta que permite la comunicación, intercambiar información y sociabilizar de manera rápida, el acceso a internet fue destinado para los adultos, pero con el paso del tiempo ahora tienen acceso los menores de edad usándola de forma positiva y otros de forma negativa.

La facilidad de conexión a la red para usarla como un medio de comunicación por las redes sociales ocasionando en algunos casos amenazas, acosos, con el fin de seducir a una persona menor de edad, la informática forense indica la causa, daño, herramientas, procesos brindando un panorama de todo lo sucedido con el fin de aplicar la ley y castigar estos delitos informáticos que se dan por el uso incorrecto de la

privacidad de la información como puede ser datos personales, no se deben publicar demasiados datos personales en internet y en caso de hacerlo utilizar la privacidad al máximo posible, en el caso de las imágenes y videos en la red se debe tener cuidado que tipo de contenido publicamos , se pierde el control y llega a ser vulnerable en el uso y la divulgación, no aceptar ni agregar a personas desconocidas que suelen engañar su identificación por gustos e intereses determinados para lograr los objetivos propuestos, por otra parte comunicar a los padres o tutores situaciones que se presentan para prevenir el cibergrooming. [1]

En esta investigación pretende determinar el marco de trabajo y las herramientas para el análisis forense en la atención de los delitos informáticos de cibergrooming bajo los dispositivos móviles Android promoviendo la seguridad de la privacidad a las personas en el uso correcto de la red de internet.

G. ALCANCE

El trabajo de la línea de investigación va orientado al análisis del perfil de celulares Inteligentes con sistema operativo Android.

H. CONCEPTOS RELACIONADOS

Grooming es una conducta de acciones que son tomadas por personas mayores de edad con el fin de ganar amistad y la confianza de personas menores es decir de niños o adolescentes con la finalidad de abusar sexualmente de este tipo de personas, esto conlleva a la pornografía infantil o prostitución. Cibergrooming es la manera de realizar las cosas por medio del internet y es utilizada por adultos como personas pederastas que se encargan de crear salas de chat, blogs, foros para tener el contacto con niños o adolescentes con la finalidad de realizar poses eróticas o de presentarse desnudos por medio de una cámara web para después con el material utilizarlo como chantaje. (Mora G. X., Metodologia de la informática forense en la atención de delitos informáticos de cibergrooming, 2015)

Delito Informático o ciberdelincuencia es toda aquella acción, típica, antijurídica y culpable que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet. Fraude Informático consiste en inducir a otra persona a hacer las cosas de manera criminal y así obtendrá un beneficio de manera económica utilizando medios informáticos. Contenido obsceno u ofensivo

indica cuando se envía mensajes a través del internet con contenido que atenta contra la integridad de una o más personas u organizaciones por medio de las redes sociales, emails etc.

[3]

El Cyberbulling consiste en el acoso entre iguales, mediante medios telemáticos, internet, chat, móvil, videojuegos, redes sociales, el daño es la victima sufre un deterioro de autoestima y dignidad personal dañando el estatus social, así como también el estrés emocional y el rechazo social, considerando el comportamiento de la intención de causar daño de modo explícito en los inicios de la acción agresora, cuenta con tres roles diferentes como es el acosador, que se realiza la acción, el acosado es quien la recibe y el observador que son todas aquellas terceras personas. Las motivaciones de los acosadores pueden ser muy variadas en casos para poder realizar el reconocimiento social derivado de un sentimiento de inferioridad sobre las personas que en este caso son víctimas. Los síntomas que pueden estar afectados son los siguientes:

-Ausencias repetidas a clase, justificadas o injustificadas.

-Bajo rendimiento escolar y dificultad para concentrarse.

-Cambios o pérdidas de amistades repentinas.

-Cambios de humores inexplicables o al mirar el móvil, correo electrónico, chats, redes sociales.

-Cambio en el patrón de uso de las nuevas tecnologías.

-Recibe llamadas o mensajes de texto al móvil que una persona se pone nerviosa.

-Dificultad para dormir, pesadillas frecuentes. [4]

Análisis Forense Informático está comprendido por un conjunto de técnicas pensadas para poder extraer la información de cualquier soporte sin alterar el estado, lo que permite identificar datos ocultos, dañados o eliminados. Esta comprendido una serie de etapas entre ellas están:

- Asegura la escena con el propósito de impedir que nadie pueda alterar algo.
- Identificación de evidencias identifican los dispositivos y sistemas a analizar evidencias importantes.
- Adquisición de datos es la fase crítica con la posibilidad de modificar errores digitales.

- Análisis de datos busca información útil en relación a las evidencias donde puede estar la información eliminada, registrada, logs del sistema, ficheros entre otros. [5]

El proceso de análisis forense móvil tiene como objetivo recuperar las evidencias digitales o datos que sean de mayor importancia de un dispositivo móvil de manera que conserve la evidencia en condición sólida, el suceso necesita reglas precisas que incauten, aíslen, transporten, almacenen para poder realizar pruebas digitales que se originen de manera segura desde dispositivos móviles. [6]

I. TRABAJOS RELACIONADOS

Para el presente proyecto se toma como referencia los siguientes trabajos y se puntualizara los temas que nos servirán.

En el año 2017, la investigación sobre la metodología de análisis forense orientada a incidentes en dispositivos móviles describe la búsqueda de evidencias almacenada en los dispositivos, bajo un escenario en el que identifica los delitos informáticos con las necesidades de tener estándares que permitan garantizar la integridad de las evidencias encontradas y a su vez permite realizar procesos forenses sobre los dispositivos móviles. Considerando en la evolución y multiplicidad del uso de los dispositivos móviles que las personas de diferentes edades realizan con determinadas horas sin considerar las políticas de seguridad y privacidad, está investigación permitirá conocer los diferentes tipos de metodología para poder realizar un análisis forense de acuerdo a la utilidad de los dispositivos móviles. [7]

En una investigación realizada en el año 2016 se mencionó acerca de los comportamientos de los adolescentes en redes sociales, por medio de la recopilación de la información que surgen de las páginas web oficinales y las páginas web que no son oficiales pero que abordan los aspectos conceptuales de manera importante considerando aspectos jurídicos y referenciales con la iniciativa de la protección de la información de los datos que se almacenan de manera insegura en las páginas que se utilizan de manera frecuente. La misma que permitirá identificar el tipo de actitud de los adolescentes en el uso de las redes. [8]

En otra investigación se manifiesta el análisis del desarrollo del fenómeno de sexting entre los adolescentes considerando la etapa de numerosos cambios que se han ido evolucionando por el uso de las redes sociales, siendo de gran influencia el uso correcto de las herramientas de apoyo para la conectividad entre las personas

ya sean con fines de amistad, de familia o con fines malintencionados por perjudicar la reputación de las personas, perjudicándoles de manera negativa ante la sociedad, por convenios ya sean económicos o de recompensaciones personales. Esta investigación accederá a identificar el uso correcto de las redes de manera óptima y segura [9]

J. METODOLOGÍA

En el presente trabajo de investigación se utilizará el método de investigación deductivo que permitirá deducir conclusiones lógicas en referencia al tema de investigación a través de la aprobación de la encuesta para proceder a la aplicación de encuestas, tabulación de los resultados obtenidos y la elaboración del artículo científico.

K. CRONOGRAMA DE ACTIVIDADES

N°	ACTIVIDAD	MES						
		I	II	III	IV	V	VI	MEDIOS DE VERIFICACIÓN
1	Analizar documentación científica e Identificar aspectos legales en el Ecuador a cerca del cibergrooming							
	Mediante documentación digital	X	X					Hojas de Excel de los links. Hoja de Excel de los Autores
2	Seleccionar la metodología que permita estructurar el proceso de extracción de información de dispositivos móviles sobre la base del delito de Cibergrooming.							
	Modelo de encuesta Validación de la Encuesta Permiso para admitir la aplicación de encuestas Realización de la encuesta		x					
3	Ejecutar pruebas sobre las herramientas que nos permita recuperar información en los dispositivos móviles utilizando técnicas de informática forense.			X				
	-Análisis de la información establecida de la tabulación de los resultados de la encuesta aplicada -Generación del artículo científico.			X	X			Hoja de Excel de la tabulación de resultados Documento en Word

L. DECLARACIÓN FINAL
Los abajo firmantes declaramos bajo juramento que el proyecto descrito en este documento no ha sido presentado a otra institución nacional o internacional para su financiamiento, no causa perjuicio al ambiente, es de nuestra autoría y no transgrede norma ética alguna.

M. PARTICIPANTES	
DIRECTOR:	Ing. Cristina Flores
ESTUDIANTE 1	Julio Murudumbay

N. FIRMAS DE RESPONSABILIDAD	
Lugar:	
Fecha:	

Firmas:

Nombre: Ing. Cristina Flores	Nombre: Julio Murudumbay
CC:0302090535	C.C.:0350160487
Director del Proyecto	**Estudiante / Egresado**

O. APROBACIÓN	
Firmas:	
Nombre:	Nombre:
CC:	C.C.:
Primer Par Revisor	**Segundo Par Revisor**

P. REFERENCIAS

Referencias

[1] S. M. Alonso, «Consejos para prevenir el Cibergrooming,» *Inesem,* vol. 4, nº 14, p. 29, 2016.

[2] G. X. Q. Mora, *Metodologia de la informática forense en la atención de delitos informáticos de cibergrooming,* Cuenca, 2015.

[3] P. Arnedo Blanco, «Herramientas de análsis forense y su aplicabilidad en la investigación de delitos informáticos,» Valledupar, 2018.

[4] J. P. Padilla, *Seguridad y Riesgos: Cyberbullying, Grooming y Sexting,* 2019.

[5] «http://www.prakmatic.com/,» Gestión, 6 Julio 2018. [En línea]. Available: http://www.prakmatic.com/seguridad-ti/que-es-el-analisis-forense-informatico/#:~:text=El%20An%C3%A1lisis%20Forense%20Inform%C3%A1tico%20comprende,determinante%20en%20un%20proceso%20judicial.. [Último acceso: 14 Junio 2018].

[6] Y. González, «Atico34,» Grupo, 3 Julio 2020. [En línea]. Available: https://protecciondatos-lopd.com/empresas/informatica-forense/. [Último acceso: 15 Mayo 2020].

[7] D. Pinto, «Metodología de análsis forense orientada a incidentes en dispositivos móviles,» *Maskana,* vol. 5, nº 24, p. 24, 2017.

[8] D. A. Villarreal, «El ciberbulling, Grooming y Sexting en la política pública Mexicana; Un tema emergente para el trabajo social.,» *AMCDC,* vol. 24, nº 61, p. 19, 2016.

[9] A. B. R. C. Marta Gordillo Hernández, «Sexting:Nuevos usos de la tecnología y la sexualidad en adolescentes,» *Psicología,* vol. 1, nº 84-99, p. 1, 2015.

[10] M. Campoverde-Molina y L. Valverde, «Accessibility analysis of the web portals of the educational institutions in Cuenca, Ecuador,» *Revista Cátedra,* vol. 2, nº 2, pp. 55-75, 2019.

[11] V. Simbaña-Gallardo y S. Luján-Mora, «Instructions about the manuscript structureof Revista Cátedra,» *Revista Cátedra,* vol. 1, nº 1, pp. 36-52, 2018.

[12] Universidad Católica de Cuenca, «Directrices para autores/as,» 2020. [En línea]. Available: https://killkana.ucacue.edu.ec/index.php/killkana_tecnico/about/submissions.

Proyecto

INFORME DE ORIGINALIDAD

8%	8%	1%	6%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Fundacion Universitaria Juan de Castellanos Trabajo del estudiante	1%
2	vsip.info Fuente de Internet	1%
3	Submitted to Aliat Universidades Trabajo del estudiante	1%
4	eujournal.org Fuente de Internet	1%
5	derechoecuador.com Fuente de Internet	1%
6	ojs.unemi.edu.ec Fuente de Internet	1%
7	Submitted to Universidad Peruana Los Andes Trabajo del estudiante	1%
8	sedici.unlp.edu.ar Fuente de Internet	1%
9	informaticaeducativaysinmiedo.blogspot.com Fuente de Internet	

1 %

Excluir citas	Activo	Excluir coincidencias	< 1%
Excluir bibliografía	Activo		

Universidad Católica de Cuenca

Pro Sciences
Revista de Producción, Ciencias e Investigación.
http://www.journalprosciences.com/index.php/ps

CONSTANCIA DE ACEPTACIÓN DE ARTÍCULO

PRO SCIENCES: REVISTA DE PRODUCCIÓN, CIENCIAS E INVESTIGACIÓN con ***ISSN: 2588-1000***, perteneciente al ***CENTRO DE INVESTIGACIÓN Y DESARROLLO PROFESIONAL***, en cabeza de su editor Joffre León-Acurio.

Hace constar:

Que, el artículo titulado: **"MARCO DE TRABAJO Y HERRAMIENTAS PARA EL ANÁLISIS FORENSE EN LA ATENCIÓN DE LOS DELITOS INFORMÁTICOS DE CIBERGROOMING BAJO LOS DISPOSITIVOS MÓVILES ANDROID"** de autoría del investigador: **Misael Julio Murudumbay Huerta**, se presentó el 28 de abril de 2022 en nuestra revista para su revisión.

Se informa que el artículo fue sometido a un proceso *double–blind_peer–review*, para verificar el cumplimento de las políticas y directrices de los autores requeridas por la revista, siendo así la decisión final, **PUBLICABLE**, mismo que se visualizará en la edición Vol. 6. N° 43 (2022) junio.

Asimismo, se declara que actualmente la revista se encuentra incluida en: ***Latindex Catálogo 2.0; REDIB (Red Iberoamericana de Innovación y Conocimiento Científico); MIAR; Actualidad Iberoamericana; ERIHPLUS (European Reference Index for the Humanities Social Sciences); OAJI (Open Academic Journals Index); LatinREV (Red Latinoamericana de Revistas Académicas en Ciencias Sociales y Humanidades); Research Bib; BASE; PKP INDEX; Open Archives; Open AIRE Explore; ISSN (International Standard Serial Number Internacional Centre); CROSSREF (Content Registration); Signatory of DORA***.

Las ediciones de la revista se encuentran publicadas en el portal de **Pro Sciences: Revista de Producción, Ciencias e Investigación** http://www.journalprosciences.com/index.php/ps

Para constancia, se firma la presente en la ciudad de Babahoyo a los 10 días del mes de mayo del año 2022.

Cordialmente,

Firmado electrónicamente por:
PRAXEDES AMERICA MONTIEL DIAZ

Ing. Práxedes Montiel-Díaz. MSc.
Directora
Pro Sciences: Revista de Producción, Ciencias e Investigación
Centro de Investigación y Desarrollo Profesional

Autorización De Publicación En El Repositorio Institucional

Misael Julio Murudumbay Huerta portador de la cedula de ciudadanía Nº **0350160487** En calidad de autor y titular de los derechos patrimoniales de trabajo de titulación **"MARCO DE TRABAJO Y HERRAMIENTAS PARA EL ANÁLISIS FORENSE EN LA ATENCIÓN DE LOS DELITOS INFORMÁTICOS DE CIBERGROOMING BAJO LOS DISPOSITIVOS MÓVILES ANDROID."** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos. Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de este trabajo de titulación en Repositorio Institucional de conformidad a los dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cañar, **13 de mayo 2022**

F: ……

Misale Julio Murudumbay Huerta

C.I. **0350160487**