25

Fecha de presentación: julio, 2020
Fecha de aceptación: septiembre, 2020
Fecha de publicación: octubre, 2020

GUÍA INTEGRAL

DE EMPLEO DE LA INFORMÁTICA FORENSE EN EL PROCESO PENAL DE ECUADOR

COMPREHENSIVE GUIDE TO THE USE OF FORENSIC INFORMATICS IN THE CRIMINAL PROCEDURE OF ECUADOR

Frankz Alberto Carrera Calderón[1]
E-mail: ua.frankzcarrera@uniandes.edu.ec
ORCID: https://orcid.org/0000-0003-4260-1608
Mario Ramiro Aguilar Martínez[1]
E-mail: ua.marioaguilar@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-6469-8335
[1] Universidad Regional Autónoma de Los Andes. Ecuador.

Cita sugerida (APA, séptima edición)

Pino Andrade, E. E., Rojas Cárdenas, J. A., & Sailema Armijo, J. G. (2020). Guía integral de empleo de la informática forense en el proceso penal de Ecuador. *Revista Universidad y Sociedad*, 12(S1), 182-190.

RESUMEN

El debido proceso sin duda constituye un principio que garantiza un resultado justo dentro de un proceso judicial, éste al encaminar la actuación de las pruebas, deja ver la autenticidad y su validez procesal. La tecnología es uno de los instrumentos que permite la expansión de la información, pero al mismo tiempo se torna vulnerable al cometimiento de ilícitos, por ello es importante que se regule a través de protocolos la compilación y guarda de las evidencias que permitirán el esclarecimiento de los hechos. Este artículo tiene como objetivo destacar los resultados principales alcanzados en el proyecto "Guía Integral de Empleo de la Informática Forense en el Proceso Penal de Ecuador y desarrollo del software de soporte" llevado a cabo por la Universidad UNIANDES de Ecuador. Dicho proyecto aplicó una estrategia basada en el trabajo realizado por UFASTA en Argentina y adaptándolo a la legislación ecuatoriana. La estrategia contiene cuatro etapas claramente definidas y con resultados parciales en cada una de ellas. Siendo una de las más destacadas la elaboración de un protocolo de peritaje de delitos informáticos.

Palabras clave: Informática, cadena de custodia, evidencias digitales, protocolo.

ABSTRACT

Due process is undoubtedly a principle that guarantees a fair outcome within a judicial process, which, by directing the performance of the evidence, reveals its authenticity and procedural validity. Technology is one of the instruments that allows for the expansion of information, but at the same time it becomes vulnerable to the commission of illicit acts. This article aims to highlight the main results achieved in the project "Comprehensive Guide to the Use of Computer Forensics in Ecuador's Criminal Procedure and Development of Support Software" carried out by UNIANDES University of Ecuador. This project applied a strategy based on the work done by UFASTA in Argentina and adapted it to the Ecuadorian legislation. The strategy contains four clearly defined stages with partial results in each of them. One of the most important is the development of a protocol for the assessment of computer-related crimes.

Keywords: Computing, chain of custody, digital evidence, protocol.

INTRODUCCIÓN

El desarrollo de las Tecnologías de Información y Comunicación (TIC) es innegable (Barranquero, 2017), esto ha permitido una integración a nivel mundial como nunca en la historia de la humanidad. Este desarrollo tiene aparejado consigo una serie de problemas, dentro de ellos, se encuentra el uso inadecuado de las tecnologías de la comunicación para cometer delitos (Rifa Pous, Serra Ruíz & Rivas López, 2009) ya que las mismas están presentes en casi todas las actividades del ser humano, así como en instituciones públicas y privadas.

De acuerdo con el criterio de Dominguez (2013), la *"parte vital en el combate contra el crimen es una investigación de medios digitales basada en métodos profesionales y buenas prácticas al efecto de que los elementos de videncia obtenidos mediante la misma puedan ser puestos a disposición de los tribunales".* De ahí que sea necesario tomar en cuenta a la Informática Forense como disciplina que se *"encarga de la adquisición, el análisis y la valoración de elementos de evidencia digital hallados en ordenadores, soportes de datos e infraestructuras de red, y que pudieran aportar luz en el esclarecimiento de actividades ilegales perpetradas en relación con instalaciones de proceso de datos".*

Este tipo de delitos en el caso ecuatoriano están normados por diferentes cuerpos legales, entre ellos se puede mencionar a la Constitución de la República (Ecuador. Asamblea Nacional Constituyente, 2008), el Código Orgánico Integral Penal (COIP) (Ecuador. Asamblea Nacional, 2014), la Ley de Comercio Electrónico, Firmas electrónicas y mensajes de datos (Ecuador. Congreso Nacional, 2002), entre otras.

De acuerdo con el informe de la Fiscalía General En Ecuador (2015), los delitos informáticos van desde el fraude hasta el espionaje, las denuncias receptadas sobre este tema fueron: 2009 – 168 casos, 2010 – 1099 casos, 2011 – 3129 casos, 2012 – 2682 casos, 2013 – 2070 casos, desde enero hasta 10 de agosto del 2014 – 877 casos, desde enero de 2015 hasta 31 de mayo del 2015 (entró en vigencia el Código Orgánico Integral Penal) – 626 denuncias. Las provincias con mayor porcentaje de incidencia de delitos informáticos fueron Pichincha 47, 38 %, Guayas 27,57, El Oro 5,24 %, estos datos fueron considerando el total de los casos hasta agosto del 2014.

El Código Orgánico Integral Penal (Ecuador. Asamblea Nacional, 2014), establece como delitos informáticos más importantes los mencionados en los artículos 173 y 174 referentes al acoso sexual y oferta de servicios sexuales con menores de edad vía medios electrónicos. Artículos del 190 al 194 que tipifican la apropiación fraudulenta de la información y dinero a través de medios electrónicos. Artículo 191 el cual considera delito a la programación o modificación de información de equipo terminales móviles (tabletas, celulares, Ipad, laptops, entre otros). Artículos del 229 al 234 que tipifican delitos que comprenden desde la interceptación ilegal de datos hasta acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

Los delitos al utilizar tecnología de punta, requieren en la mayoría de los casos para su investigación personal especializado, para recabar todos los elementos de convicción necesarios y así establecer la responsabilidad de la infracción como del infractor, estas evidencias requieren un tratamiento especial desde el proceso de búsqueda, obtención, preservación, examen pericial y presentación de evidencias digitales (Ecuador. Asamblea Nacional, 2014; Narváez-Montenegro, et al., 2015). Por otro lado, no solo es necesario una persona que sea perito en el tema, sino que se debe contar con hardware y software que permita desarrollar dicho trabajo y, lo más importante contar con un protocolo claro, cuidando la cadena de custodia para su pleno y eficaz valor procesal.

La Fiscalía General de Estado (2014), elaboró el Reglamento del Sistema Especializado Integral de Investigación, de Medicina Legal y Ciencias Forenses (RSEIIMLCF), publicado en el Registro Oficial mediante Resolución FGE-2014-030 y Manuales, Protocolos, Instructivos y Formatos Del Sistema Especializado Integral De Investigación Medicina Legal y Ciencias Forenses, publicado en el Registro Oficial mediante Resolución No. 073-FGE-2014, el cual establece los protocolos a seguir para la investigación de los delitos, los mismos que pese a su volumen y cantidad, en la práctica resultaron ambiguos y mucho más en los delitos informáticos.

Por otra parte, la Universidad FASTA (UFASTA)de Argentina, desarrolló el Proyecto PAIF-PURI (Protocolo de Actuación en Informática Forense a partir del Proceso Unificado de Recuperación de Información), el mismo que tiene como objetivo el desarrollo de un Protocolo de Actuación en Informática Forense para ser adoptado y promovido por el Ministerio Público de la Provincia de Buenos Aires como estándar oficial de trabajo.

Dicho proyecto basa su funcionamiento por lo establecido en el Proceso Unificado de Recuperación de Información (PURI), oportunamente desarrollado por el Grupo de Investigación en Informática Forense y Sistemas Operativos de la Facultad de Ingeniería de la UFASTA. Luego UFASTA desarrolló el proyecto "Guía Integral de Empleo de la Informática Forense en el Proceso Penal" (Luz, et al., 2013; Di Iorio, 2016).

En los años 2012 y 2013 UNIANDES desarrolló proyectos de investigación con la transferencia y colaboración del grupo de investigación de Informática Forense de la Universidad FASTA de Argentina, proyectos que dieron un inicio para que el proyecto Guía Integral de Empleo de la Informática Forense en el Proceso Penal, sea replicado en el Ecuador, ya que Ecuador cuenta con una normativa jurídica, una realidad social, económica y cultural diferente a la Argentina, que implica una investigación propia tanto en el área informática como en el derecho.

METODOLOGÍA

Para el desarrollo de la investigación que dio como resultado el presente artículo se planteó tres etapas que se detallan en la figura 1.

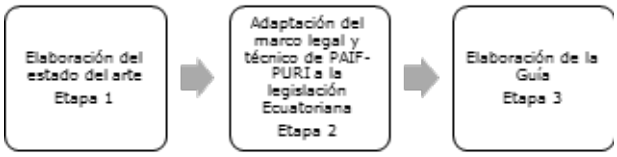

Figura 1. Estrategia seguida para la elaboración de Guía Integral de Empleo de la Informática Forense en el Proceso Penal.

En una primera etapa se realizó un proceso de revisión bibliográfica (Gálvez Toro, 2001), en el mismo se recopiló y analizó documentos existentes sobre delitos informáticos, su investigación y procedimiento de juzgamiento en la legislación ecuatoriana, con el fin de desarrollar el estado del arte.

Dentro del grupo de temas investigados de forma bibliográfica para generar el estado del arte proyecto se puede mencionar las siguientes: 1) actuación pericial en el Código Orgánico Integral Penal; 2) facultades de la fiscalía; 3)sistema especializado integral de investigación de medicina legal y ciencias forenses; 4) informes periciales; 5) delitos informáticos; 6) protocolo de actuación informático forense; 7) adquisición de datos volátiles; 8) cadena de custodia y preservación de muestras y pericias; 9) adquisición de medios de almacenamiento persistentes; 10) labores periciales; 11) evidencias en medios tecnológicos; 12) acta de levantamiento de soporte de evidencia digital, técnicas y herramientas de informática forense; 13) aspectos legales y estratégicos del empleo de la informática forense en el proceso penal; 14) la informática forense en el proceso penal; 15) cuestiones de jurisdicción y competencia; 16) cooperación internacional; 17) intervenciones en el reconocimiento del lugar de los hechos y finalmente 18) destino de las evidencias.

Como fuente básica de estudio se tuvo: 1) la Constitución de la República del Ecuador, el Código Orgánico Integral Penal (COIP); 2) la Ley de Comercio Electrónico, Firmas electrónicas y mensajes de datos; 3) Reglamento del Sistema Especializado Integral de Investigación, de Medicina Legal y Ciencias Forenses (RSEIIMLCF); 4) manuales, protocolos, instructivos y formatos del Sistema Especializado Integral de Investigación Medicina Legal y Ciencias Forenses; 5) diferentes obras de prestigiosos autores sobre el tema y 6) Ley Orgánica de Entidades de seguridad.

Para la segunda etapa se realizó un proceso de análisis y síntesis de los documentos generados por UFASTA que son base del proyecto: 1) PAIF-PURI: Guía Integral de Empleo de la Informática Forense en el Proceso Penal; 2) PURI: Proceso Unificado de Recuperación de la Información (PURI + PURI en Redes + PURI en Smartphone).

En la tercera etapa se procedió a sintetizar y formalizar el conocimiento generado a partir de la legislación ecuatoriana y la documentación de UFASTA, adaptando los puntos que fueron necesarios para crear la Guía Integral de Empleo de la Informática Forense en el Proceso Penal.

DESARROLLO

El proyecto ha alcanzado una serie de resultados en su proceso de ejecución, dentro de ellos se pueden mencionar los siguientes:

Análisis del marco legal ecuatoriano.

La Constitución la República (Ecuador. Asamblea Nacional Constituyente, 2008) en su Art. 167 menciona que ***"la potestad de administrar justicia emana del pueblo y se ejerce por los órganos de la Función Judicial y por los demás órganos y funciones establecidos en la Constitución".*** Por otra parte, el Art. 178, establece que los órganos jurisdiccionales son los encargados de administrar justicia y son: 1) la Corte Nacional de Justicia; 2) las cortes provinciales de justicia; 3) los tribunales y juzgados que establezca la ley; 4) los juzgados de paz; además en el mismo articulado se menciona que el Consejo de la Judicatura es el órgano de gobierno, administración, vigilancia y disciplina de la Función Judicial.

El Art. 178 considera que la Fiscal General del Estado es un órgano autónomo de la Función Judicial y el Art. 195 de la Constitución de la República (Ecuador. Asamblea Nacional Constituyente, 2008) dice que "***corresponde a la Fiscalía dirigir de oficio o a petición de parte, la investigación pre-procesal y procesal penal"***; además la Fiscalía debe organizar y dirigir un sistema especializado integral de investigación, de medicina legal y ciencias forense.

En concordancia con el Art. 178 de la Constitución del Ecuador, el Art. 443 numeral 1 del Código Orgánico Integral Penal, sobre las atribuciones de la Fiscalía le atribuye la organización y dirección del sistema especializado integral de investigación de medicina legal y ciencias forenses.

Un aspecto importante que destacar del Art. 443 del Código Orgánico Integral Penal (Ecuador. Asamblea Nacional, 2014) está dado en su numeral tres, ya que le atribuye a la Fiscalía la capacidad de expedir en coordinación con las entidades que apoyen al sistema especializado integral de investigación, de medicina legal y ciencias forenses, los manuales de procedimiento y normas técnicas para el desempeño de las funciones investigativas.

De igual manera, el Reglamento del Sistema Especializado Integral de Investigación de Medicina Legal y Ciencias Forenses- ***RSEIIMLCE*** (Ecuador. Fiscalía General del Estado, 2014), expedido el 11 de abril de 2014, contiene todas las disposiciones que regulan la organización, implementación y dirección del Sistema, para la correcta aplicación de manuales, instructivos y protocolos de Medicina Legal en la investigación pre-procesal y procesal penal.

Dentro de las atribuciones de la o el fiscal en el numeral 12 y 14 del Art. 444 del Código Orgánico Integral Penal está la de ordenar el peritaje integral de todos los indicios que hayan sido levantados en la escena del hecho, garantizando la preservación y correcto manejo de las evidencias y disponer la práctica de las demás diligencias investigativas que considere necesaria.

El sistema especializado integral de investigación, de medicina legal y ciencias forenses, de acuerdo con el Art. 448 del Código Orgánico Integral Penal debe ser organizado por la Fiscalía, contará con el apoyo del organismo especializado de la Policía Nacional y personal civil de investigación. Las atribuciones que el sistema especializado integral de investigación tiene están instituidos en el Art. 449.

El Título IV del Código Orgánico Integral Penal denominado "Prueba" establece cual es la finalidad de la prueba, así como los principios que rigen el anuncio y práctica de la prueba. Dentro del principio de igualdad de oportunidades para la prueba está definido la "Cadena de Custodia" en el Art. 456.

Además, el Art. 456 menciona que son responsables de la aplicación de la cadena de custodia, el personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, el personal competente en materia de tránsito y todos los servidores públicos y particulares que tengan relación con estos elementos, incluyendo el personal de servicios de salud que tengan contacto con elementos físicos que puedan ser de utilidad en la investigación.

La preservación de la escena del hecho o indicios está determinada por el Art. 458 del Código Orgánico Integral Penal, y establece que *"la o el servidor público que intervenga o tome contacto con la escena del hecho e indicios será la responsable de su preservación, hasta contar con la presencia del personal especializado. Igual obligación tiene los particulares que por razón de su trabajo o función entren en contacto con indicios relacionados con un hecho presuntamente delictivo".*

Las actuaciones y técnicas especiales de investigación están contempladas en los artículos 459 al 497. Las actuaciones de investigación y las diligencias de reconocimiento constarán en actas e informes periciales. El reconocimiento del lugar de los hechos cuando sea relevante para la investigación por parte de la o el fiscal con el apoyo del personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, se lo realizará de acuerdo con lo que está establecido en el Art. 460 del Código Orgánico Integral Penal. El numeral 8 del Art. 460 menciona que *"se realizarán diligencias de reconocimiento del lugar de los hechos en territorio digital, servicios digitales, medios o equipos tecnológicos".* (Ecuador. Asamblea Nacional, 2014).

El Art. 470 del Código Orgánico Integral Penal (Ecuador. Asamblea Nacional, 2014) menciona que la información obtenida ilegalmente carece de todo valor jurídico. Por otra parte, la correspondencia física, electrónica o de cualquier otro tipo o forma de comunicación es inviolable, salvo los casos expresamente autorizados (Art. 475). La intercepción de las comunicaciones o datos informáticos se encuentra fijado bajo los parámetros dados en el Art. 476 del Código Orgánico Integral Penal

El Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público (Ecuador. Asamblea Nacional, 2014) en su Art. 145, indica la participación de otras entidades con el Servicio Nacional de Medicina Legal y Ciencias Forenses dentro del ámbito de su competencia entre ellos se encuentran, el Cuerpo de Vigilancia Aduanera, Cuerpo de Bomberos, Cuerpo de Vigilancia de la Comisión de Tránsito del Ecuador y otras entidades de conformidad a la Ley, con sujeción a las directrices y resoluciones emitidas por el Comité Directivo y bajo la coordinación operativa de la Policía Nacional.

Como se mencionó anteriormente la Fiscalía tiene la potestad de general manuales, protocolos, instructivos y formatos del sistema especializado integral de investigación, medicina legal y ciencias forenses, para dar cumplimiento a esto mediante Registro Oficial No 318 del 25 de

agosto del 2014, se expidió la Resolución No. 073-FGE-2014. En él se encuentra la sección denominada Área de cadena de custodia y dentro de ella el manual de cadena de custodia. El punto 4 de esta manual habla sobre el instructivo para el manejo de indicios y/o evidencia digital.

De igual forma, mediante Registro Oficial No 225 del 14 de abril del 2014, se expide el Reglamento del Sistema Especializado Integral de Investigación, de Medicina Legal y Ciencias Forenses (Ecuador. Asamblea Nacional, 2017). Siendo estos fundamentales para el trabajo en la parte de informática forense.

La tabla 1, establece los principales delitos informáticos de acuerdo con el Código Orgánico Integral Penal (Ecuador. Asamblea Nacional, 2014).

Tabla 1. Principales delitos informáticos establecidos en el Código Orgánico Integral Penal y tipología.

Artículo	Tipo de delito informático
178. Violación a la intimidad. Pena privativa de libertad de 1 a 3 años.	• Datos falsos o engañosos. • Falsificaciones informáticas. • Fishing. • Fuga de datos. • Parasitismo informático. • Suplantación de personalidad.
186. Estafa. Pena privativa de libertad de cinco a siete años.	• Falsificaciones informáticas. • Manipulaciones de datos de salida. • Fishing.
190. Apropiación fraudulenta por medios electrónicos. Pena privativa de libertad de uno a tres años.	• Transferencia ilícita de dinero. • Datos falsos o engañosos. • Técnica del salami. • Manipulaciones de datos de salida. • Fishing. • Gusanos. • Virus informáticos. • Malware. • Ataque de negación de servicio. • Parasitismo informático. • Suplantación de personalidad.
212. Suplantación de identidad. Pena privativa de uno a tres años.	• Fishing. • Parasitismo informático. • Suplantación de personalidad.
229. Revelación ilegal de base de datos. Pena privativa de uno a tres años.	• Fuga de datos. • Hurto del tiempo del computador.
230. Interceptación ilegal de datos. Pena privativa de tres a cinco años.	• Datos falsos o engañosos. • Manipulación de datos de salida. • Fishing. • Puertas falsas. • Llave maestra.
231. Transferencia electrónica de activo patrimonial. Pena privativa de tres a cinco años.	• Transferencia ilícita de dinero. • Técnica del salami. • Falsificaciones informáticas.
232. Ataque a la integridad de sistemas informáticos. Pena privativa de libertad de tres a cinco años. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana pena privativa de libertad de cinco a siete años.	• Datos falsos o engañosos. • Caballo de Troya. • Bombas lógicas. • Gusanos. • Virus informáticos. • Malware. • Ataques de negación de servicios. • Puertas falsas, • Llave maestra.
234. Acceso no consentido aun sistema informático, telemático o de telecomunicaciones. Pena privativa de libertad de tres a cinco años.	• Hurto del tiempo del computador. • Llave maestra.

Guía Integral de Empleo de la Informática Forense en el Proceso Penal de Ecuador.

La Guía Integral de Empleo de la Informática Forense en el Proceso Penal de Ecuador, se basa en la guía creada por la UFASTA de Argentina, adaptada al marco legal ecuatoriano.

La guía consta de:

- Consideraciones generales.

- Evidencia digital (Art. 500 COIP).
- Roles y niveles de actuación procesal.
  - Rol de asesoramiento. (Art. 11 RSEIIMLCF).
  - Rol investigative (Art. 442 COIP), (Art 6, 7,8,11 RSEIIMLCF).
  - Rol pericial (Art. 457, 511 COIP); (Art. 6,7,8,11 RSEIIMLCF).
- Principios generales en el manejo de evidencia digital. Relevancia, suficiencia, validez legal y confiabilidad (Art. 458, 471 COIP).
  - Confiabilidad, justificable, auditable, repetible y reproducible (Art. 505 COIP, Art. 511 COIP).
- Procedimiento de consulta (Art. 10 RSEIIMLCF).
- Fases de intervención del informático forense (Art. 449 COIP), (Art. 13,14,15,16,17,18 RSEIIMLCF).
  - Relevamiento e identificación de equipos, dispositivos o medios de almacenamiento.
  - Recolección de equipos, dispositivos o medios de almacenamiento. Adquisición de datos volátiles.
  - Cadena de custodia y preservación.
  - Adquisición de medios de almacenamiento persistentes.
  - Labores periciales.

Se trabaja con el modelo PURI desarrollado por UFASTA.

- Relevamiento e identificación.
  - Consiste en la identificación de los equipos, dispositivos y todo otro tipo de medio de almacenamiento cuya obtención y/o examen se considere pertinente y útil para aspectos específicos del plan de investigación penal delineado en un caso concreto por el Fiscal y/o su equipo.
  - Medios de identificación.
  - Cuestiones de jurisdicción y competencias. (Art. 13 RSEIIMLCF).
  - Perfil del responsable de identificación. (Art. 442, 511 COIP), (Art. 11 RSEIIMLCF).
  - Pedidos de medidas de injerencia. (Art 13, 14 RSEIIMLCF).
- Recolección.
  - Principios básicos de actuación.
  - Objetivo.
  - Procedimiento. (Art. 13 RSEIIMLCF).
  - Registración. (Art. 14 RSEIIMLCF)
  - Variables que considerar: preparación; actuación en equipo; aseguramiento de la prueba; inspección de la escena y de los dispositivos; evidencias y personas vinculadas con los artefactos a recolectar; evidencias a recolectar; manipulación y levantamiento de los objetos; recomendaciones para la clasificación, embalaje y rotulado; documentación y registro de lo actuado; recaudos adicionales para teléfonos móviles.
  - Adquisición de datos no volátiles.
  - Criterios especiales de actuación: aseguramiento; inspección; manipulación, alteración y/o destrucción de datos; orden de levantamiento de datos; identificación de datos; acceso a datos; registro; documentación y validación.
- Cadena de custodia y preservación (Art. 456 COIP).
  - Principios básicos de actuación.
  - Recaudos especiales.
- Adquisición de medios de almacenamiento persistentes.
  - Preparación y desarrollo de las tareas.
  - Inspección y manipulación.
  - Tarea de adquisición (Art. 460 COIP).
  - Documentación (Art. 499 COIP).
  - Cadena de custodia. (Art. 292, 456 COIP), (Resolución No. 073-FGE-2014).
- Labores periciales (Art. 450, 511 COIP).
  - Marco procesal e institucional. Principios de actuación.
  - Deber de reserva.
  - Límites legales.
  - Etapas.
  - Actos y formalidades iniciales.
- Consultas y consultas previas.
  - Análisis (447 COIP).
  - Interpretación.
  - Elaboración del dictamen pericial (Art. 499, 459, 467, 511 COIP).

Entendiendo que el objetivo de establecer la cadena de custodia como un conjunto de actividades y procedimientos secuenciales, consiste en la protección y aseguramiento de los indicios y/o evidencias tanto físicas como digitales desde la localización en la escena de la infracción hasta su presentación ante los juzgados competentes, y que permite o facilita el esclarecimiento de actos delictivos y la responsabilidad de éstos; es importante, manifestar que a través del derecho comparado existen procesos coincidentes entre sí y otros que se suman con la finalidad de completar los protocolos establecidos para el efecto.

Según la legislación argentina, se considera como evidencia digital a cualquier información que, sujeta a una intervención humana, electrónica y/o informática, ha sido extraída de cualquier clase de medio tecnológico informático (computadoras, celulares, aparatos de video digital, etc.). Técnicamente, es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales. La evidencia digital presenta características que la diferencian de las restantes clases de evidencia física. Se la puede duplicar de manera exacta (permitiendo manipular la réplica sin alterar el original), está sujeta a riesgos específicos de posible alteración y/o eliminación, su localización puede ser muy dificultosa, por tal consideración se hace indispensable que los protocolos para la recolección y conservación de estas evidencias sean efectivos y eficaces a través de procesos claros, específicos y concretos.

No sólo se hace importante, el proceso sino también la infraestructura, es decir la legislación debe prever que, a más del protocolo, existe un espacio físico y/o digital seguro que permite conservar los indicios y/o evidencias intactas hasta llegar a los juzgados pertinentes.

Los recursos humanos utilizados dentro del proceso deben ser peritos en su área, es decir, deben contar con los conocimientos bastos y suficientes que garanticen la correcta investigación de los hechos y que permitan encausar a una decisión acertada por los órganos competentes.

Un protocolo de esta naturaleza debe necesariamente, estar fundamentado en principios que garanticen el cumplimiento del o los objetivos para los que fue creado, en cuanto a esto y comparando la legislación ecuatoriana y argentina se diferencian y a la vez se complementan con el aporte que cada una hace, así dentro de los principios ecuatorianos tenemos: garantía, responsabilidad, registro, preservación y verificación versus la legislación argentina: relevancia, suficiencia, validez legal, confiabilidad. Todos estos complementarios y dirigidos a saber discriminar la necesidad de la evidencia y la pertinencia de la misma dentro del caso que se investiga.

Una vez que se han establecido las bases sobre las cuales la evidencia digital va a ser compilada para luego ser expuesta, es ineludible el delineamiento de pasos a seguir, así: en el Ecuador, los procesos o fases van desde el manejo de la escena, ingreso al centro de acopio, traspaso, transporte, análisis, embalaje y sellado de las evidencias hasta los jueces competentes. En lo que respecta a Argentina, los procesos van desde las fases de identificación, recolección, adquisición de datos volátiles, preservación, adquisición de medios persistentes y laborales periciales. Cada uno de los mencionados con sus especificidades que permiten que los peritos e investigadores y todas las personas que actúan dentro de la compilación de evidencias, una vez que los conocen, garantizar su seguro traslado al espacio físico adecuado para la conservación de las mismas.

De la cadena de custodia, otro de los aspectos relevantes es la facultad del perito y/o investigador, en base a sus conocimientos y experiencia, de poder escoger acertadamente la escena que va a ser investigada y las pruebas que discriminará y considerará conducentes y oportunas; esto permite, racionalizar los recursos que invierten los estados para la realización del trabajo en esta área de análisis.

Tanto en Argentina como en el Ecuador, lo que se trata es de garantizar el debido proceso, el derecho a la contradicción, la celeridad procesal a través de la correcta recolección de evidencias, todo ello nos lleva a concluir que, cumpliendo los protocolos en base a los principios, las evidencias cuentan con legalidad y validez procesal, lo que las hace indispensables en la solución de delitos.

Las Constituciones de los Estados garantizan que la actuación procesal, bajos sus principios, goce de transparencia y legalidad, que la actuación de las partes intervinientes en el proceso se encauce a la solución del problema, sin embargo, es necesario que las legislaciones se adecuen a los cambios y a las nuevas formas de cometimiento de actos delictivos.

El camino a la globalización nos acerca cada vez a la necesidad de reformar la legislación para poder sancionar los delitos que ahora se producen a través de la tecnología.

Sabiendo que el ciberespacio es un mundo complejo, de gran capacidad de almacenamiento de información, pero a la vez vulnerable a la violación del mismo, las seguridades de los estados se ven sensibles ante los actos delictivos cada vez más complejos y que requieren

la organización y desarrollo de protocolos de aplicación interestatal que garantice al menos un proceso seguro de recolección y conservación de evidencia digital que ha servido como base para el cometimiento de ilícitos.

El personal encargado de las cadenas de custodia debe necesariamente, preparase continuamente con la finalidad de que estos sean capaces de lograr el objetivo a ellos encomendado en cuanto a discriminación de evidencias y selección de escenas del ilícito, que garanticen un verdadero aporte al sistema judicial.

Entendiendo la complejidad a la que la legislación se enfrenta y estudiando lo ya existente sobre cadena de custodia de evidencia digital, se deduce que si bien existen protocolos que deben ser revisados a nivel internacional, que permitan la construcción de una guía que garantice la aplicación de procesos claros, seguros, eficaces sobre la recolección y conservación de evidencias, que despejen en lo más posible la manipulación o destrucción de las mismas con la finalidad de evadir responsabilidad judicial.

El presente trabajo ha tenido como objetivo analizar y comparar dos legislaciones (ecuatoriana y argentina) sobre el tema en cuestión, teniendo como resultado que el ecuador necesita adecuar un proceso que garantice la recolección y conservación de evidencias. Argentina cuenta con el protocolo que podría servir de base para esclarecer un proceso eficaz.

El Ecuador requiere aporte y cooperación que le permita la preparación del recurso humano en el tema de delitos informáticos y la compilación de pruebas. Un gran intento fue el inicio del protocolo existente sobre cadena de custodia, sin embargo, se hace necesario analizarlo, compáralo y adecuarlo a las necesidades presentes y futuras en cuanto a la evolución de los actos delictivos.

La falta de protocolos claros sobre cadena de custodia puede acarrear la ineficacia de la norma, pues al no tener garantías claras sobre las pruebas que se considerarán para acusar o no a un sujeto, la impunidad será el día a día de la justicia.

El aporte que las legislaciones internacionales como la Argentina en el caso que nos ocupa, será de gran valor en base a un esfuerzo conjunto, llegar a la aplicación eficaz de la ley y el esclarecimiento de hechos delictivos que no suceden en un espacio físico visible para todos, sino más bien en un mundo digital, desconocido para muchos, en donde los códigos y los accesos no están al alcance de todos y donde las autoridades deberán entenderlo, conocerlo y reconocerlo para la aplicación eficaz de la justicia.

La existencia de un protocolo que refleje el proceso sobre la obtención y guarda de las evidencias garantiza que las mismas gocen de autenticidad y con ello tengan el valor probatorio dentro del proceso que se investiga a la vez, se vislumbra la imparcialidad del estado a través de los órganos competentes e intervinientes e n el esclarecimiento de los hechos y la determinación de la culpabilidad.

El diseño y construcción de un espacio que permita custodiar las evidencias sobre el cometimiento de delitos a través de medios informáticos es uno de los aspectos importantes y relevantes para el éxito y cumplimiento de los procedimientos y conclusión del objetivo trazado dentro de los procesos judiciales.

Este trabajo es sin duda un reto en países como el ecuador en donde el sistema judicial cada vez se reestructura o se reforma, lo importante es marcar los lineamientos sobre los cuales esta novedad jurídica debe caminar, será necesario capacitar constantemente a todos aquellos funcionarios sobre los cuales recae la responsabilidad de garantizar el debido proceso en todas sus etapas, desafío éste, que permitirá dar pasos sólidos encaminados a los cambios constantes de un mundo cada vez más globalizado, en donde el uso de la tecnología desafía la aplicación de la justicia.

CONCLUSIONES

El desarrollo de las Tecnologías de Información y Comunicación (TIC) es innegable, esto ha permitido una integración a nivel mundial como nunca antes en la historia de la humanidad. La parte vital en el combate contra el crimen es una investigación de medios digitales basada en métodos profesionales y buenas prácticas al efecto de que los elementos de videncia obtenidos mediante la misma puedan ser puestos a disposición de los tribunales

Los delitos al utilizar tecnología de punta requieren en la mayoría de los casos para su investigación personal especializado, para recabar todos los elementos de convicción necesarios y así establecer la responsabilidad de la infracción como del infractor, estas evidencias requieren un tratamiento especial desde el proceso de búsqueda, obtención, preservación, examen pericial y presentación de evidencias digitales

La legislación ecuatoriana no ha desarrollado los protocolos necesarios para garantizar de forma completa el proceso de peritaje en cuanto se refiere a delitos informáticos.

Las Constituciones de los Estados garantizan que la actuación procesal, bajos sus principios, goce de transparencia y legalidad, que la actuación de las partes intervinientes en el proceso se encauce a la solución del

problema, sin embargo, es necesario que las legislaciones se adecuen a los cambios y a las nuevas formas de cometimiento de actos delictivos.

La estrategia desarrollada por el grupo de trabajo del proyecto garantizó alcanzar los resultados requeridos por dicho proyecto, ya que permitió establecer los fundamentos jurídicos que se relacionan a los delitos informáticos en Ecuador, así como establecer una comparativa entre la legislación argentina y ecuatoriana en la parte de delitos informáticos.

El trabajo conjunto entre UFASTA y UNIANDES permitió generar un trabajo activo entre los diferentes técnicos que se involucraron en dicho proyecto.

REFERENCIAS BIBLIOGRÁFICAS

Barranquero, M. F. (2017). Sociedad del conocimiento, tecnología y educación. TE & ET: Revista Iberoamericana de Tecnología en Educación y Educación en Tecnología, 19(97).

Di Iorio, A.H. (2016). Guía Integral de Empleo de la Informática Forense en el Proceso Penal. Universidad FASTA.

Domínguez, F. L. (2013). Introducción a la informática forense. Grupo Editorial RA-MA.

Ecuador. Asamblea Nacional Constituyente. (2008). Constitución de la República. Registro Oficial N. 446. https://www.ambiente.gob.ec/wp-content/uploads/downloads/2018/09/Constitucion-de-la-Republica-del-Ecuador.pdf

Ecuador. Asamblea Nacional. (2014). Código Orgánico Integral Penal. Registro Oficial N. 180. https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf

Ecuador. Asamblea Nacional. (2017). El Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público. Registro Oficial N. 19. https://www.igualdadgenero.gob.ec/wp-content/uploads/2018/05/C%C3%B3digo-Org%C3%A1nico-de-Entidades-de-Seguridad-Ciudadana-y-Orden-P%C3%BAblico.pdf

Ecuador. Congreso Nacional. (2002). Ley de Comercio electrónico, firmas y mensajes de datos. Registro Oficial N. 557. https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

Ecuador. Fiscalía General del Estado. (2014). Reglamento del Sistema Pericial Integral de investigación, de medicina legal y ciencias forenses. Registro Oficial N. 225. https://www.fiscalia.gob.ec/wp-content/uploads/2012/04/files_LOTAIP%20AC_Reglamento_del_Sistema_Especializado_Integral_de_Investigacin_de_Medicina_Legal_y_Ciencias_Forenses.pdf

Ecuador. Fiscalía General del Estado. (2015). Los delitos informáticos van desde el fraude hasta el espionaje. FGE. https://www.fiscalia.gob.ec/los-delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje/

Gálvez Toro, A. (2007). Enfermería Basada en la Evidencia. Cómo incorporar la investigación a la práctica de los cuidados. Fundación Index.

Luz Clara, B., Di Iorio, A. H., Urirarte, V., Giaccaglia, M. F., & Navarro, E. (2013). Defensa del consumidor en la contratación de bienes y servicios informáticos. Fasta.

Narváez-Montenegro, D., Fiallos, S., Bucaram, A., Viscaino, F., & Carrera-Calderón, F. A. (2015). Derecho Informático. Concepto, principios y prácticas. Editorial Jurídica del Ecuador.

Rifa Pous, H., Serra Ruíz, J., & Rivas López, J. R. (2009). Análisis Forense de los Sistemas Informáticos. Eureca Media.