MAESTRÍA EN AUDITORIA DE TECNOLOGÍAS DE LA INFORMACIÓN

ANÁLISIS DE BRECHAS DEL PROCESO DE COMPUTACIÓN FORENSE EN ECUADOR RESPECTO A LAS BUENAS PRÁCTICAS INTERNACIONALES.

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por las estudiantes:
Doris María MERA MERO
Vaneza Mariana Benavides Córdova

Bajo la dirección de:
Washington Antonio CEVALLOS GAMBOA

Universidad Espíritu Santo
Maestría en Auditoría de Tecnologías de la Información
Samborondón - Ecuador
Abril del 2018

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

Analysis of gaps in the process of forensic computing in Ecuador regarding good international practices.

Doris María MERA MERO[1]
Vaneza Mariana Benavides Córdova[2]
Washington Antonio CEVALLOS GAMBOA[3]

Resumen

Este artículo se centra en determinar el nivel de madurez del proceso de computación forense en Ecuador respecto a las buenas prácticas internacionales. Para lo cual, basados en la metodología Delphi se seleccionaron cinco peritos informáticos calificados por el Consejo de la Judicatura del Ecuador, experimentados en casos de análisis forenses y pertenecientes a varias ciudades del país. Así mismo, haciendo uso de la metodología Science Design se crearon instrumentos que permitieron recabar la información proporcionada por los expertos. Por ello, a partir de la información analizada se puede concluir que en la actualidad Ecuador está ubicado en el nivel dos de madurez, siendo la etapa de presentación la de mayor puntuación y la etapa de manejo de expedientes la de menor puntuación, lo cual indica que dentro del proceso de análisis forense ejecutado en el país los procedimientos están siendo implementados, pero aun necesitan ser documentados y estar en mejora continua.

Palabras clave: Informática forense, evidencia digital, peritaje informático, funcion judicial, análisis de brechas

Abstract

This article focuses on determining the level of maturity of the forensic computing process in Ecuador with respect to international good practices. For this purpose, based on the Delphi methodology, five computer experts qualified by the Judicial Council of Ecuador, experienced in forensic analysis cases and belonging to several cities of the country, were selected. Likewise, using the Science Design methodology, instruments were created that allowed gathering the information provided by the experts. Therefore, from the information analyzed it can be concluded that currently Ecuador is located at level two of maturity, the presentation stage being the highest score and the record management stage the lowest score, which indicates that within the process of forensic analysis executed in the country the procedures are being implemented, but still need to be documented and be in continuous improvement.

Key words: Computer forensics, digital evidence, computer expertise, judicial function, gap analysis

INTRODUCCIÓN

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

La creación de la computación forense surge de los avances paralelos de los dispositivos informáticos, los cuales han abierto al mundo criminal un sin fin posibilidades para la ejecución de actividades ilícitas donde el anonimato ha hecho que sea atractivo cometer delitos lejos del lugar del crimen, dificultando así la labor de la justicia.

Es por ello, que según una encuesta ejecutada por el Servicio Secreto de Estados Unidos[USSS] en 1995, el 70% de los organismos policiales estaban ejecutando análisis forenses sin un manual de procedimientos.

Es así que, según ISACA (2015) el FBI organizó la Conferencia Internacional sobre la aplicación de la Ley de la evidencia en el ordenador donde el grupo G8 dispuso la *Guía internacional de Principios y Protocolos para la Evidencia Digital,* que permitió que la evidencia digital sea aceptada en los tribunales.

Así pues, según The Hill (2017) en el año 2017 se firmó en Estados Unidos el apoyo al proyecto denominado "Fortalecimiento de la Ley de Lucha contra el Delito Cibernético Local 2017", el cual autoriza al Instituto Nacional de Informática Forense a la educación de funcionarios estatales y locales de Estados Unidos en la búsqueda de pruebas digitales en todo tipo de delitos, bajo la convicción de que en la era actual casi todos los delitos involucran algún tipo de evidencia digital.

Por otro lado, algo semejante ocurrió en Argentina, donde a partir del 2014 tomó mayor impulso el Proceso Unificado de Recuperación de la Información desarrollado por el Grupo de Investigación en Informática Forense de la Universidad de la Fraternidad de Agrupaciones Santo Tomás de Aquino [FASTA], la cual dio paso a la elaboración de la Guía Integral de Empleo de la Informática Forense en el Proceso Penal, la misma que fue finalizada, aprobada y puesta en marcha por la Procuración General de la Provincia de Buenos Aires en el año 2016 (Di Lorio, 2016).

Así mismo, según señala Piaccirilli (2015) existen otros estudios que han fijado su atención en el desarrollo de protocolos en base a la evidencia digital y al uso de herramientas de software libre dentro del proceso forense, a partir de lo cual para el año 2016 y 2017 las investigaciones han sido orientadas al diseño de laboratorios que soporten la evaluación de la calidad de los procesos periciales y a la revisión sistémica de buenas prácticas para la recolección de la evidencia (Armilla, Panizzi, Eterovic, & Torres, 2017).

Por otra parte, en el contexto colombiano, se han identificado esfuerzos en la realización de metodologías de análisis forense en Linux según lo indican Santos & Flores (2013), por lo que se han propuesto frameworks para la computación forense enmarcado en las leyes colombianas (Álvarez, Marín, & Victoria, 2012). Así mismo, ´según Buitrago (2014) se ha propuesto la viabilidad de la implementación de un laboratorio de informática forense en la ciudad de Pereira encaminando los esfuerzos a nuevos retos para la informática forense como el manejo de la evidencia en iPhone 3G (Ariza, Ruiz, & Cano, 2009).

Por otro lado, uno de los países que también se unió al tratamiento de la evidencia digital es España, ante lo cual según el Informe Nacional de la Policía Científica de España (2011), en el primer trimestre del año 2010 la Policía Científica elaboró un Manual de normas de procedimientos en Pericias Informáticas, que daba respuesta a los cambios constantes dados en el análisis de los dispositivos, pretendiendo ser adaptado a nuevas realidades de tal manera que garantice la labor de los especialistas y la confianza por parte de los jueces o fiscales hacia la labor pericial. Es así, que en el año 2010 se llegaron a realizar 1.100 informes periciales a nivel nacional y posteriormente en el

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

año 2015 según el Ministerio de Interior de España se obtuvieron 1.359 peticiones de análisis forense.

Es por ello, que en la actualidad cada perito informático perteneciente a la Policía Científica tiene a su disposición un ordenador forense personal con cada una de las herramientas que le permitan realizar su labor y efectuar los análisis a su cargo haciendo uso del manual que los rige.

Sin embargo, la Asociación de Tasadores y Peritos Judiciales Informáticos (2017) señala que existe la gran necesidad de capacitación respecto al tema, experiencia práctica en la aplicación de metodologías, elaboración de informes, oratoria, defensa pericial y actualización permanente por parte de los peritos informáticos.

Por otro lado, Ecuador inició el recorrido en este campo a partir del año 2014 donde según Guerra (2014) se han abordado temas como análisis y aplicación de software para recuperación forense de evidencia digital en dispositivos Android. Por su parte, Bolaños & Gómez (2015) plantearon un estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador basados en casos procesales, proponiendo la inclusión de nuevos tipos de evidencias digitales dentro del análisis, así mismo, Loarte & Lima (2017) propusieron para el año 2017 contar con un Marco de trabajo estandarizado para el análisis forense de la evidencia digital**.**

Es de esta manera, que según señala Fernández (2004) se ha podido reflejar la falta de procedimientos y estándares dentro del manejo de la evidencia digital, a lo cual agrega que la forma de obtener y almacenar las evidencias está basada en las buenas maneras que cada perito considera más no en fundamentaciones teóricas que permitan asegurar el debido proceso. De la misma forma, Montoya (2010) indica que la falta de capacitación y adaptación de las nuevas tendencias es también uno de los problemas que avoca actualmente dentro del campo de la informática forense. Ante ello, Padilla (2014) expresa que al ser la informática forense una ciencia reciente algunos países entre ellos Uruguay aún no existen normas que regulen estos procesos.

Es por ello que el presente proyecto de titulación permitirá determinar el nivel de madurez del proceso de computación forense en Ecuador respecto a las buenas prácticas internacionales mediante el análisis de brechas que ayudará a conocer el estado actual en el que se encuentra el país, proponer acciones para llegar al estado deseado, crear conciencia entre los involucrados de la necesidad de seguir un procedimiento formal que le brinde fiabilidad a los casos procesales y poder evidenciar la necesidad de tener personal capacitado.

MARCO TEÓRICO

ANÁLISIS FORENSE

Según detalla Vera (2017) la informática forense surge como respuesta a la necesidad de investigar crímenes realizados haciendo uso de medios informáticos, así pues, en 1978 el estado de Florida de Estados Unidos reconoce el sabotaje, pornografía, obtención y borrado de datos entre otros como delitos relacionados a la tecnología.

Seguidamente, en 1984 el Departamento Federal de Investigaciones [FBI] creó el Programa de medios magnéticos que actualmente es conocido como Computer Analysis and Response Team [CART] el cual según indica Villamil (2014) llegó a analizar 17 terabytes de datos hasta 1999.

Así mismo, en 1995 como consecuencia del surgimiento de la informática forense se creó la Organización Internacional de Evidencia Digital [IOCE] la cual según Rodríguez & Doménech (2011) tenía la finalidad de compartir la

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

información que estuviese relacionada con las buenas prácticas de análisis forense alrededor del mundo.

De esta manera, Córdova (2014) revela que en diciembre de 1997 el grupo denominado G8 dio a conocer que aquellos funcionarios que estén a cargo de hacer cumplir la ley deben tener los conocimientos propios y a su vez hacer uso de aquellos equipos sofisticados para hacer frente a los delitos de alta tecnología. De igual forma, en marzo de 1998 el mismo grupo fue nombrado para crear los principios internacionales relacionados a la evidencia digital (Córdova, 2014).

Así pues, en la actualidad la informática forense mediante las estandarizaciones de los procedimientos que ésta conlleva ya es aplicada en diversos campos, como, por ejemplo, para la persecución de criminales donde se toman en consideración las evidencias digitales y de esta manera conocer la conducta delictiva (Rojas, 2017).

De la misma manera, es aplicada en el ámbito civil donde se pueden descubrir acoso, difamaciones, infidelidades entre otros en base a la evidencia adquirida (Rojas, 2017).

Otro campo que lo utiliza son los seguros, en el cual mediante análisis de pruebas dentro de dispositivos para los reclamos o compensaciones que se presenten (Rojas, 2017)

Por otro lado, varios autores han empezado por definir esta rama de la ciencia enfocada hacia varios ámbitos, por ello, Constantini, De Gasperis, & Olivieri (2015) define el análisis forense como una rama de la criminología que promueve la identificación, adquisición, preservación, análisis y presentación del contenido de la información de los sistemas informáticos o en general de dispositivos digitales.

Por su parte, Alharbi, Weber, & Traore (2011) indican que es la capacidad de recoger, preservar y analizar pruebas para identificar a un incidente que se produzca. Ante lo cual, Carrol, Brannon & Song (2008) agregan que este debe ser ejecutado mediante herramientas y métodos comprobados científicamente que permitan al perito reconstruir o analizar los hechos que hayan sido encontrados, de tal manera que la evidencia digital sea ubicada, reproducida y analizada para trámites legales.

METODOLOGÍAS DE ANÁLISIS FORENSE

La Real Academia Española (2010) define la palabra metodología como “un conjunto de métodos que son implementados con el fin de realizar una investigación científica”.

Ante lo cual, Pesada (2012) destaca que hacer uso de ella permite desarrollar actividades estandarizadas de una manera lógica y ordenada que pueden ser interpretadas por cualquier individuo conocedor del tema.

Por ello, para el análisis de la computación forense según Rodríguez & Doménech (2017) existen un sin números de metodologías que han surgido por diversas organizaciones, las cuales están enfocadas en cubrir las etapas que conlleva este proceso según el tipo de aplicación que se le dé. Entre las metodologías aplicadas constan:

ISO 27042:2015

Según detalla Cano (2015) la Organization Standard International [ISO] con el afán de dar respuesta las necesidades informáticas forenses crearon la ISO 27042:2015, la cual mediante un marco de buenas prácticas asegura que las actividades realizadas en las investigaciones forenses se ejecutan de manera equivalente.

Por ello, ISO/IEC (2015) expresa que la ISO 27042:2015 está relacionada particularmente al análisis forense de la forense. La figura 1 evidencia las etapas conformadas.

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

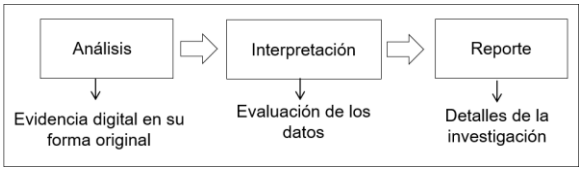


Figura 1: Etapas de la norma ISO 27042:2015
Fuente: Elaboración de las autoras

DEPARTAMENTO DE JUSTICIA DE ESTADOS UNIDOS

National Institute of Justice (2001) indica que esta guía fue creada para el uso por parte de los encargados de hacer cumplir la ley y otros miembros de la comunidad que sean responsables del examen de las pruebas digitales.

Para ello, cubre las etapas de: Preparación o extracción, identificación, análisis y conclusión, donde en cada una de ellas se describen los pasos necesarios para realizar un análisis forense informático y sugerir el orden en que deben llevarse a cabo. La figura 2 muestra las etapas que esta metodología conlleva.

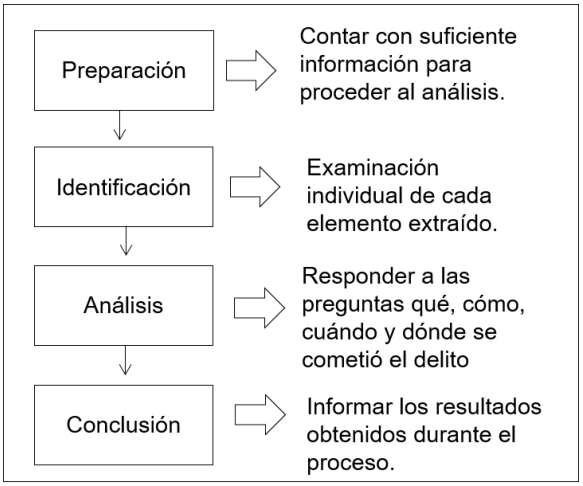


Figura 2: Etapas de la norma del Departamento de Justicia de Estados Unidos.
Fuente: Elaboración de las autoras

INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA

Según expresa NIST (2006) esta metodología fue desarrollada basada en el cumplimiento de sus responsabilidades bajo la Ley Federal de Administración de la Seguridad de la Información[FISMA] del 2002. Dicha metodología permite desarrollar la capacidad forense en conjunción con una amplia orientación proporcionada por asesores legales, funcionarios encargados de hacer cumplir la ley y el proceso de gestión para la realización del análisis forense, el mismo que se basa en ejecutar la recolección haciendo uso de los medios, la revisión basados en datos, el análisis de la información y el reporte de las evidencias analizadas.

Por su parte, también agrega que ésta proporciona información detallada sobre cómo utilizar el proceso de análisis con cuatro grandes categorías de fuentes de datos: archivos, sistemas operativos, tráfico de red y las aplicaciones. De esta manera la figura 3 evidencia las fases.

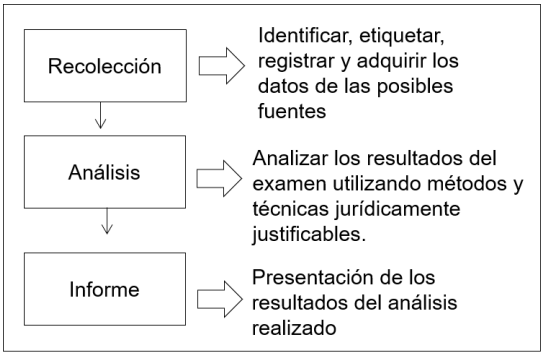


Figura 3: Etapas de la norma NIST
Fuente: Elaboración de las autoras

UNE 71506:2013

Según detalla la Asociación Española de Normalización y Certificación (2011) la UNE 71506:2013 fue elaborada por el comité técnico AEN/CTN 71 y consta de 23 páginas.

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

Así mismo, la norma en referencia junto con la UNE 71505, son muy utilizadas por profesionales, organismos, fuerzas y cuerpos de seguridad del estado español; cuyo objetivo es obtener resultados válidos en un proceso forense. La figura 3 muestra las etapas compuesta por la metodología UNE 71506:2013

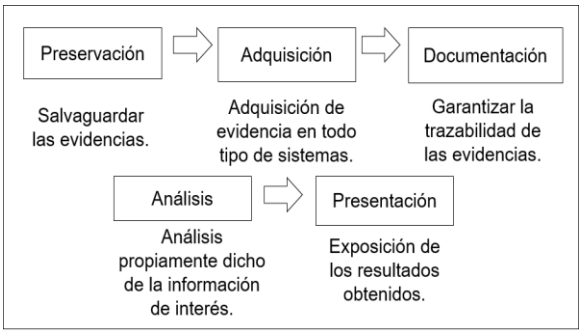


Figura 4: Etapas de la metodología UNE 71506:2013
Fuente: Elaboración de las autoras

GUIA INTEGRAL DE EMPLEO DE LA INFORMÁTICA FORENSE EN EL PROCESO PENAL DE ARGENTINA

Lerena, Di Lorio, Podestá & Constanzo (2015), manifiestan que la única guía Argentina consignada a orientar a profesionales de la informática forense y organismos judiciales en el proceso de obtener una evidencia digital válida, es la Guía Integral de empleo de la Informática Forense en el proceso penal; la misma que fue aprobada por la procuradora de la Suprema Corte de la Provincia de Buenos Aires bajo la resolución general 483/16 en el 2016.

Así pues, esta guía se presenta dividida en seis fases no necesariamente vinculadas de forma secuencial, con lo cual se presentan los aspectos básicos a considerar en las labores relacionadas a la informática forense. La figura 5 muestra estas etapas.

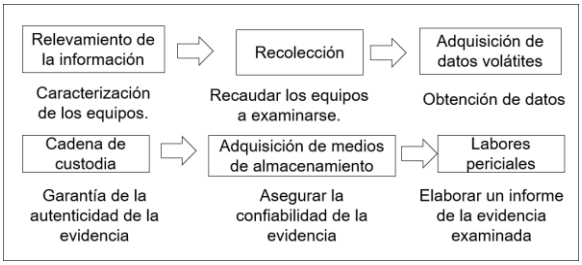


Figura 5: Etapas de la Guía Argentina.
Fuente: Elaboración de las autoras

EVIDENCIA DIGITAL

Rodríguez & Doménech (2011) manifiestan que a inicios de los años 90 el FBI determinó que la evidencia digital gozaba del potencial para convertirse en un elemento probatorio tan poderoso en la lucha contra la delincuencia, es así que a finales de los 90 inicia el impulso del manejo de este tema con el fin de desarrollar principios aplicables a los procedimientos para tomar acciones sobre la evidencia digital.

Ante este antecedente han surgido referencias como la norma ISO/IEC 27037:2012, que proporciona pautas para el manejo de la evidencia digital, y actualmente la ISO/IEC 27042 que se enfoca en el análisis e interpretación de la misma, con el propósito de mantener la integridad de la evidencia digital con fines de contribuir a su admisibilidad en procesos legales. (Roatta, Casco, & Fogliato, 2012).

En este contexto la evidencia digital de acuerdo a Cano (2012) puede ser dividida en tres categorías: 1. Registros recopilados en el equipo de tecnología informática como correos electrónicos, archivos de aplicaciones de ofimática, imágenes, entre otros., 2. Registros creados por los equipos de tecnología informática como es el caso de registros de auditoría, registros de transacciones, registros de eventos, etc. y 3. Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática como las hojas de cálculo financieras, consultas

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

especializadas en bases de datos, vistas parciales de datos, etc.

Así pues, al ser la evidencia digital la materia prima de un investigador es necesario detallar las características que la hacen parte fundamental del proceso, Cano. (2016), menciona que la evidencia digital es un desafío para quienes la analizan debido al contexto variable por lo que debe ser volátil, anónima, duplicable, alterable y eliminable.

Con lo antes mencionado, son diversas las definiciones que surgen en esta temática, según Amaya (2012) la evidencia digital es una copia del documento original, el mismo que está almacenado en un archivo; en el cual se debe considerar que las copias obtenidas sean exactas a las originales para lograr la validez de la evidencia.

De acuerdo con Carrier & Spafford (2004), la evidencia digital es la razón por la que una investigación digital inicia, la misma que incluye un examen digital para la recolección de pruebas.

Por otro lado, Ćosić, & Bača (2011) indican que la evidencia digital se define como cualquier dato almacenado para ayudar a resolver cómo se dieron los hechos en un proceso legal.

De la misma manera, Rodríguez & Doménech (2011) agregan que la evidencia digital es toda información de valor probatorio que se almacena en forma digital.

Ante ello Locard (2014) ratifica que dos objetos que entran en contacto siempre transfieren material que involucra al otro, tal como se evidencia en la figura 6.

Figura 6: Interacción de la evidencia digital
Fuente: Locard (2014)

METODOLOGÍA.

Haciendo uso del método de investigación Delphi que según indican García Valdés & Suárez Marín (2013) permite la recolección sistemática del juicio de expertos sobre un problema en un área específica; se seleccionaron cinco peritos informáticos de las ciudades de Quito, Cuenca, Loja y Guayaquil; los mismos, que debieron cumplir los siguientes criterios: Estar acreditado como perito informático, haber participado en procesos de análisis forense digital, tener mínimo un año de experiencia y pertenecer o ser prestador de servicio del Consejo de la Judicatura del Ecuador. La tabla 1 refleja detalladamente los perfiles de los peritos entrevistados.

Ciudad	Tipo de perito	Experiencia	Título Universitario	Casos atendidos
Guayaquil	Policía	1 año	Ingeniero en Sistemas	Más de 6
Loja	Prestador de servicios	3 años	Ingeniero en Sistemas y Telecomunicaciones	Más de 6
Cuenca	Prestador de servicios	2 años	Ingeniero en Sistemas	Más de 6
Quito	Prestador de servicios	6 años	Ingeniero en Sistemas	Más de 6
Loja	Prestado de servicios	2 años	Ingeniero en Sistemas	Más de 6

Tabla 1: Perfiles de los peritos entrevistados
Fuente: Encuesta realizada a los peritos informáticos.

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

Por otro lado, respecto a la selección de los instrumentos a utilizar se optó por entrevistas online de tipo abiertas, debidamente validadas por expertos de las ramas de psicología e informática, las mismas que tuvieron la finalidad de recoger valoraciones comentadas, determinar las metodologías a incluir y conocer los ítems comunes entre los expertos.

Así mismo, haciendo uso de la metodología Science Design que está orientada a la creación de instrumentos exitosos mencionando como principio fundamental el conocimiento, comprensión de un problema y su solución; se crearon los siguientes instrumentos a utilizarse en la presente investigación.

Matriz de actividades ejecutadas por los peritos informáticos del Consejo de la Judicatura del Ecuador

Este instrumento fue realizado basado en las encuestas ejecutadas a los peritos calificados de tal manera que se pudieran obtener las actividades realizadas para proceder a escoger las metodologías de análisis forense que tienen mayor asociación al proceso ejecutado.

Matriz de selección de las metodologías de análisis forense

Esta matriz consistió en registrar el cumplimiento o no de las actividades abordadas por la metodología del Departamento de Justicia de Estados Unidos, el Instituto de Estándares y Tecnologías, el EC-COUNCIL, la Guía Integral de Empleo de la Informática Forense en el Proceso Penal de Argentina, la Red Europea de Institutos forenses, la UNE 71506:2013 Y la ISO/IEC 27042:2015 respecto a las actividades ejecutadas por los peritos informáticos del Consejo de la Judicatura del Ecuador, de tal manera que se escojan los cinco mayores puntajes de ellas para el futuro análisis.

Para ello se hizo uso de la valoración 0 y 1, en donde 1 representa el cumplimiento de la actividad y 0 el no cumplimiento. Posteriormente, se representó mediante el diagrama circular los resultados obtenidos.

Lista de revisión de las actividades comunes entre los peritos

Este instrumento contiene las actividades enmarcadas en las metodologías en estudio y tiene la finalidad de conocer el cumplimiento o no de cada una de ellas respecto a lo ejecutado por los peritos partícipes de la investigación; obteniendo de esta manera de forma específica cada procedimiento realizado dentro del análisis forense ecuatoriano.

Matriz de las actividades de las metodologías escogidas.

Esta lista de revisión fue desarrollada basada en las actividades contempladas en cada una de las metodologías escogidas, las mismas que fueron ubicadas ordenadamente en las etapas determinadas, como: Previa, preservación, adquisición, análisis, presentación y etapa final.

Lista de revisión del análisis de brechas ejecutado.

El análisis de brechas fue ejecutado basado en la escala propuesta por la metodología GAP análisis ISO 90001:2015 que según indica ISO Tool (2016) permite detectar las brechas entre el desempeño actual de la organización y el que se quiere conseguir mediante la aplicación de una calificación del 0 al 4 con la finalidad de poder fijar prioridades en cuanto a la focalización de esfuerzos del plan de acción a implementar.

Para ello, 0 (0%) significa que el proceso no existe, 1 (25%) que el proceso está establecido, 2 (50%) que el proceso está implementado, 3 (75%) que el proceso es mantenido y existen documentos y 4 (100%) que el proceso está en mejora continua.

Posteriormente, para la ejecución del cálculo individual y por ámbitos del nivel de madurez se procedió a calcular el promedio ponderado de

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

cada una de las valoraciones obtenidas y basado en ello se hizo una aproximación del siguiente nivel de madurez que se espera obtener.

PRESENTACIÓN DE RESULTADOS

Como resultado de la encuesta realizada fue posible determinar que el proceso de análisis forense ejecutado por los peritos informáticos de la Fiscalía General del Ecuador está basado principalmente en la metodología del Departamento de Justicia de Estados Unidos (13.5%), Instituto de Estándares y Tecnologías (12.9%), UNE 71506:2013 (15.3), ISO/IEC 27042:2015 (14.1%) y la Guía Integral Argentina (16.5%). Ver figura 3 y Anexo A.

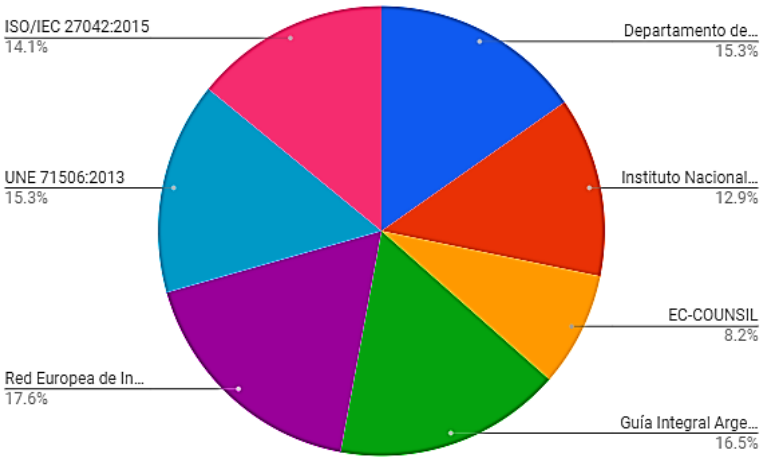


Figura 6: Metodologías del proceso de análisis forense
Fuente: Elaboración propia basada en la encuesta a peritos informáticos.

Seguidamente, una vez conocidas las metodologías en las que se basa el proceso forense ecuatoriano se establecieron los ámbitos y actividades que cada una conlleva obteniendo de esta manera la lista de revisión de la Tabla 2.

Item	Actividades	Metodologías
	Etapa previa: Certificación de la estructura y recursos requeridos	
0.1	Conocer las políticas de seguridad que posee la organización en aspectos como control de acceso a las máquinas y dispositivos, existencia o no de un registro de eventos, conocimiento de un plan de auditorías periódicas, conocimiento del sistema de gestión o control de las copias de los datos.	UNE 71506:2013
0.2	Revisar los procesos y prácticas de análisis forenses actuales y en base a ello, identificar las deficiencias de la normativa, errores de procedimiento y otras cuestiones que deben ser subsanadas, manteniendo la tendencia de la tecnología y los cambios de ley.	Instituto Nacional de Estándares y Tecnología

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

0.3	Determinar qué proceso legal adicional puede ser necesario continuar la búsqueda si llegase a encontrar una evidencia que no estaba autorizada en la orden fiscal	Departamento de Justicia de Estados Unidos
0.4	Supervisar la cadena de custodia previa hasta la llegada de las evidencias al entorno de análisis forense	UNE 71506:2013
0.5	Preparar un plan de investigación documentada que ayude a la determinación de los recursos, la selección de los procesos y herramientas para orientar al equipo de investigación	ISO IEC 27043
0.6	Realizar una labor previa de localización de las evidencias que confirme la existencia de un incidente y las causas que lo originaron	UNE 71506:2013
0.7	Actualizar periódicamente a los examinadores forenses con las últimas herramientas y técnicas que abordan las últimas tecnologías.	Instituto Nacional de Estándares y Tecnologías
0.8	Evaluar el nivel de destreza de los usuarios informáticos involucrados	Departamento de Justicia de Estados Unidos
0.9	Determinar qué tipos de datos se recogen mejor por los funcionarios encargados de hacer cumplir la ley.	Instituto Nacional de Estándares y Tecnologías
0.10	Validar y confirmar los procesos que implican el uso de nuevos instrumentos antes de la implementación.	ISO IEC 27042
0.11	Tener un kit de herramientas forenses para la recolección de datos, examen y análisis	Instituto Nacional de Estándares y Tecnologías
0.12	Conocer el objetivo, alcance y destinatarios que tendrá la investigación	ISO IEC 27042
0.13	Comprobar que el objeto y alcance de lo que se precisa estudiar está dentro de la competencia del entorno forense	UNE 71506:2013
0.14	Incluir un documento de recepción y registro de la evidencia recibida	UNE 71506:2013
0.15	Redactar el detalle de las informaciones recibidas y las decisiones que se toman, incluidos los motivos de la decisión.	ISO IEC 27042
0.16	Ejecutar el proceso de análisis forense mediante un proceso consistente.	Instituto Nacional de Estándares y Tecnologías
0.17	Poseer protocolos detallados que aseguren la integridad de las evidencias objeto del estudio forense	UNE 71506:2013
0.18	Asegurar la independencia de las actuaciones forenses, preferible con un fedatario público que de fe del proceso	UNE 71506:2013
0.19	Verificar el funcionamiento del sistema informático del examinador que incluye hardware y software	Departamento de Justicia de Estados Unidos
0.20	Contar con un esquema de codificación de los casos investigados o en investigación que refleje su identificación, fecha de inicio y finalización, orden de llegada, estado entre otros.	
0.21	Contar con conjuntos separados formal y técnicamente de equipos e infraestructura para la parte administrativa y para la parte de laboratorios de investigación forense.	
	Ámbito 1: Preservación	
1.1	Impedir el acceso no autorizado y a la alteración de las pruebas.	Instituto Nacional de Estándares y Tecnología
1.2	Designar a una persona como custodio de pruebas, donde tenga la responsabilidad exclusiva de fotografiar, documentar y etiquetar cada elemento que se recoge, y registrar cada acción	Instituto Nacional de Estándares y Tecnología

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

	que se realizó junto con quien realiza la acción, dónde fue realizado y en qué momento	
1.3	Fotografiar y grabar en video la escena de interés	UNE 71506:2013
1.4	Manipular las evidencias con la indumentaria adecuada, especialmente adaptada para evitar descargas electrostáticas.	UNE 71506:2013
1.5	Efectuar un estudio del área física y reconocer las posibles fuentes de datos.	Instituto Nacional de Estándares y Tecnología
1.6	Determinar el número y tipo de equipos en la escena	Departamento de Justicia de Estados Unidos
1.7	Documentar la ubicación desde el cual los medios fueron retirados.	Departamento de Justicia de Estados Unidos
1.8	Aislar los sistemas pertinentes de influencias externas para prevenir mayores daños al sistema.	Instituto Nacional de Estándares y Tecnología
1.9	Documentar los detalles de cada una de las pruebas encontradas antes y durante el proceso de análisis forense	Departamento de Justicia de Estados Unidos
1.10	Crear una lista de todos los usuarios que tienen acceso a los equipos que están siendo analizados para que puedan proporcionar sobre el lugar de alguna información importante.	Instituto Nacional de Estándares y Tecnología
1.11	Evaluar la necesidad de proporcionar alimentación eléctrica continua para aparatos que funcionan con pilas.	Departamento de Justicia de Estados Unidos
1.12	Si el equipo detectado como evidencia está conectado a una red se deben desconectar los cables.	Instituto Nacional de Estándares y Tecnología
1.13	Utilizar fuentes de datos alternativas si no es posible recopilar datos de una fuente primaria.	Instituto Nacional de Estándares y Tecnología
1.14	Almacenar la evidencia digital en soportes adecuados antes y durante el análisis para garantizar la integridad.	UNE 71506:2013
1.15	Sellar en soportes adecuados todas las evidencias encontradas, hasta que se active su análisis por los peritos dentro del laboratorio de análisis forense para garantizar la integridad.	UNE 71506:2013
	Ámbito 2: Adquisición	
2.1	Crear un plan que priorice las fuentes de datos	Instituto Nacional de Estándares y Tecnología
2.2	Establecer el orden en que los datos van a ser adquiridos	Instituto Nacional de Estándares y Tecnología
2.3	Documentar cada paso ejecutado en la adquisición de los datos	Instituto Nacional de Estándares y Tecnología
2.4	Determinar los posibles tipos de pruebas que se persiguen	Departamento de Justicia de Estados Unidos
2.5	Adoptar los principios de la cadena de custodia al soporte de la información adquirida, acompañada de la obtención de un código hash para posterior validación.	Guía Integral Argentina
2.6	Crear un acta de levantamiento de evidencia digital	Guía Integral Argentina
2.7	Localizar todos los equipos inalámbricos determinando todos los modos de comunicación que usan éstos	UNE 71506:2013
2.8	Documentar el estado del dispositivo como marca, modelo, tamaño, configuración, ubicación, MAC, tarjeta de red entre otros que se consideren fundamentales.	Departamento de Justicia de Estados Unidos
2.9	Fotografiar y etiquetar las pruebas para proporcionar recordatorios visuales de la configuración del equipos y	Instituto Nacional de Estándares y Tecnología

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

	periféricos.	
2.10	Desconectar los dispositivos de almacenamiento para evitar la destrucción, deterioro o alteración de los datos.	Departamento de Justicia de Estados Unidos
2.11	Si se detecta que el dispositivo está accediendo a datos remotos, archivos encriptados o con claves de acceso, correspondencia o comunicaciones electrónicas, datos de carácter personal entre otros se debe consultar al responsable del procedimiento acerca de los límites que pudieran existir para la captura de la información.	Guía Integral Argentina
2.12	Buscar en dicho entorno todo tipo de notas asociadas a las palabras de paso y al PIN de acceso a los equipos	UNE 71506:2013
2.13	Hacer uso de herramientas de adquisición de datos confiables	Instituto Nacional de Estándares y Tecnología
2.14	Activar la protección contra escritura para preservar y proteger la evidencia original.	Departamento de Justicia de Estados Unidos
2.15	Estimar el valor probable relativo de cada fuente potencial de datos	Instituto Nacional de Estándares y Tecnología
2.16	Determinar lo más rápido posible si la volatidad de los datos debe ser preservada.	Instituto Nacional de Estándares y Tecnología
2.17	Seguir un procedimiento de adquisición documentado y utilizar herramientas de hardware y software reconocidas en el ámbito forense	UNE 71506:2013
2.18	De forma previa el disco duro usado para guardar el clonado forense debe ser sometido a un borrado seguro y estar dentro de su vida útil	UNE 71506:2013
2.19	Realizar dos resúmenes digitales (hash) de la información contenida en el disco duro de forma simultánea al proceso de clonado, usando herramientas de hardware o software contrastadas en el ámbito forense y verificar que ambos resúmenes sean los mismos.	UNE 71506:2013
2.20	Procurar la menor alteración y /o destrucción de datos informáticos; de darse el caso debe precisar en forma documentada en que ha consistido la alteración y cuáles son los efectos sobre el material probatorio adquirido.	Guía Integral Argentina
2.21	Realizar una copia maestra y una copia de trabajo, y trabajar sobre la copia maestra.	Instituto Nacional de Estándares y Tecnología
2.22	Ejecutar el levantamiento de los datos acorde al previo análisis de niveles de relevancia o prioridad, del tipo de dispositivo y del orden de volatilidad de la información.	Guía Integral Argentina
2.23	Verificar la integridad de los datos adquiridos	Instituto Nacional de Estándares y Tecnología
2.24	Discutir si otros procesos forenses tienen que llevarse a cabo sobre la evidencia	Departamento de Justicia de Estados Unidos
2.25	Analizar la posibilidad de emprender otras vías de investigación para obtener más pruebas digitales	Departamento de Justicia de Estados Unidos
2.26	Determinar información adicional que puede ayudar a resolver el caso	Departamento de Justicia de Estados Unidos
	Ámbito 3: Análisis	
3.1	Establecer el orden de prioridad de la prueba que se va a examinar	Departamento de Justicia de Estados Unidos

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

3.2	Mantener notas contemporáneas detalladas y precias de las cada actuación ejecutada y los procesos que estas demandaron.	ISO IEC 27042
3.3	Comprobar que las evidencias no están deterioradas y son susceptibles de su estudio forense	UNE 71506:2013
3.4	Identificar los tipos de archivos desconocidos para determinar su valor en la investigación	Departamento de Justicia de Estados Unidos
3.5	Revisar los encabezados de los archivos	Instituto Nacional de Estándares y Tecnología.
3.6	Especificar la hora de la BIOS del equipo informático en donde van instalados los discos duros que contienen la información de interés	UNE 71506:2013
3.7	Revisar los registros del sistema y de las aplicaciones que puedan estar presentes como registros de error, registros de instalación, conexión de registros, registros de seguridad entre otros.	Departamento de Justicia de Estados Unidos
3.8	Revisar los sellos de fechas y hora que figura en el sistema de archivos de metadatos para vincular archivos de interés.	Departamento de Justicia de Estados Unidos
3.9	Examinar la estructura de partición del disco para determinar si todo el tamaño físico de la unidad de disco duro se contabiliza.	Departamento de Justicia de Estados Unidos
3.10	Revisar nombres de archivos relevantes y patrones	Departamento de Justicia de Estados Unidos
3.11	Examinar las relaciones entre archivos	Departamento de Justicia de Estados Unidos
3.12	Estudiar la documentación adjunta a las evidencias	UNE 71506:2013
3.13	Considerar nuevas evidencias relevantes en el proceso que no habían sido contempladas en un principio, iniciando nuevamente la reseña de éstas, generando un nuevo proceso de gestión, custodia y trazabilidad.	UNE 71506:2013
3.14	Informar a quien solicitó el peritaje si se encuentra nuevas evidencias del incidente y esperar por nuevas instrucciones	ISO IEC 27042
	Ámbito 4: Presentación	
4.1	Ubicar la identidad de la agencia/departamento/unidad y perito(s) que ejecutaron el análisis forense.	Departamento de Justicia de Estados Unidos
4.2	Ubicar el número identificador del caso, la fecha de recepción del caso y la fecha del informe	Departamento de Justicia de Estados Unidos
4.3	Incluir la naturaleza de los hechos investigados, la ubicación donde ocurrió la incidencia, el objetivo de la investigación, los miembros del equipo de investigación junto a sus funciones, la duración de la investigación, la ubicación de la investigación, los detalles de las pruebas digitales que se han observado durante la investigación.	ISO IEC 27042
4.4	Incluir una declaración clara del escritor que participó en la investigación.	ISO IEC 27042
4.5	Usar una plantilla de informe con formato estandarizado para ayudar a garantizar que existe suficiente información incluida en los mismos.	ISO IEC 27042
4.6	Detallar la información general de los dispositivos analizados, tales como marca, modelo, número de serie entre otros.	Departamento de Justicia de Estados Unidos
4.7	Describir brevemente las medidas adoptadas durante el examen, tales como búsquedas de cadenas, búsquedas de	Departamento de Justicia de Estados Unidos

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

	imágenes, gráficos y recuperar archivos borrados	
4.8	Describir los programas utilizados en el análisis de la evidencia	Departamento de Justicia de Estados Unidos
4.9	Detallar las técnicas utilizadas	Departamento de Justicia de Estados Unidos
4.10	Informar si las pruebas digitales han tenido cualquier daño	ISO IEC 27042
4.11	Determinar los resultados y conclusiones del caso.	Departamento de Justicia de Estados Unidos
4.12	Incluir las limitaciones de cualquier análisis realizado	ISO IEC 27042
4.13	Incluir las recomendaciones para continuar con la investigación o trabajos futuros.	ISO IEC 27042
	Etapa final: Manejo de expedientes	
5.1	Mantener una copia de la orden judicial emitida por el fiscal o juez con el expediente del caso.	Departamento de Justicia de Estados Unidos
5.2	Mantener una copia de la cadena de custodia	Departamento de Justicia de Estados Unidos
5.3	Documentar las irregularidades y las medidas tomadas durante el examen	Departamento de Justicia de Estados Unidos
5.4	Almacenar a largo plazo la información confidencial capturada por herramientas forenses, asegurándose que esto no infringe la privacidad de los involucrados.	Departamento de Justicia de Estados Unidos

Tabla 2: Lista de revisión de las actividades de las metodologías de análisis forense en estudio.
Fuente: Elaboración propia de las autoras.

De la misma manera, haciendo uso de la lista de revisión anteriormente mencionada se procedió a ejecutar el análisis de brechas de cada una de las actividades propuestas mediante la cual se pudo conocer la situación actual del proceso de análisis forense que está siendo ejecutado en el Ecuador.

Es así que en las etapas estudiadas se obtuvieron los niveles de madurez que se pueden observar en la Tabla 1.

Cálculo de madurez por ámbitos	
Ámbitos	**Nivel de madurez**
Etapa previa: Certificación de la estructura y recursos requeridos	2,2
Ámbito 1: Preservación	2,6
Ámbito 2: Adquisición	2,3
Ámbito 3: Análisis	2,0
Ámbito 4: Presentación	3,4
Etapa final: Manejo de expedientes	2,0
Nivel de Madurez General	2,4

Tabla 1: Niveles de madurez alcanzados
Fuente: Elaboración propia de las autoras

Por otro lado, fue posible representar gráficamente mediante el uso del diagrama de arañas el nivel actual y esperado de cada ámbito, actividad y general. Para ello, la figura 9 muestra el detalle.

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

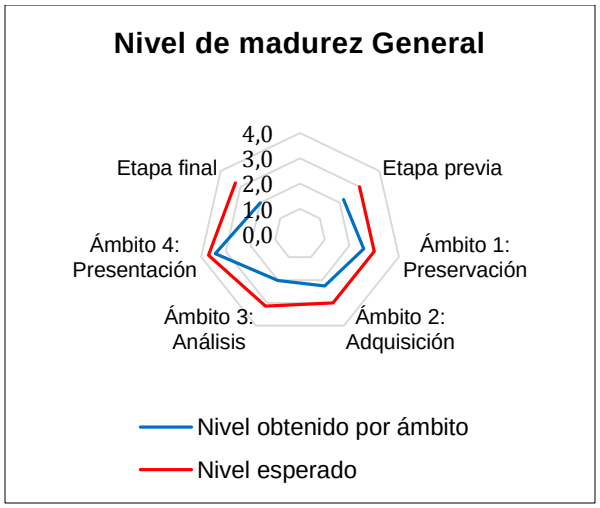


Figura 9: Nivel de madurez general
Fuente: Elaboración propia de las autoras

Por su parte en la etapa previa se determinó que en la actualidad en el análisis forense ejecutado en Ecuador no se hace uso de fedatarios públicos que den fe del proceso, los peritos se limitan a seguir y cumplir el procedimiento estipulado en el Reglamento del sistema pericial integral de la función judicial, no se identifica las deficiencias de la normativa, la cadena de custodia no es supervisada desde el estado previo hasta la llegada de las evidencias al entorno de análisis forense, la hoja de registro es enviada para ser firmada solo a las personas que manipulan la evidencia y los expertos localizan solo los dispositivos a analizar en la escena del crimen. Ver figura 10.

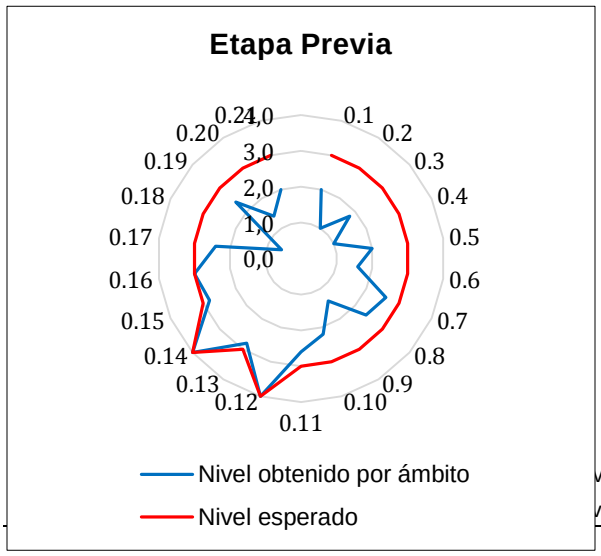
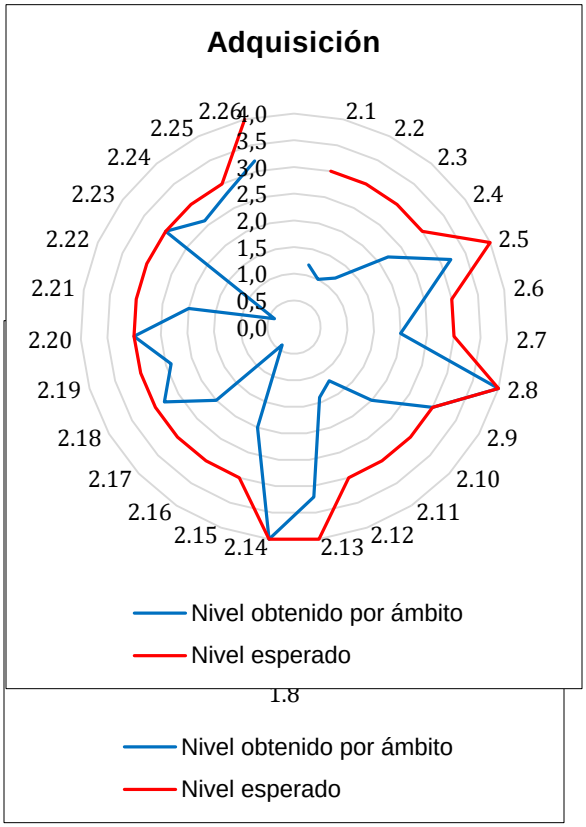


Figura 10: Niveles de madurez Etapa previa
Fuente: Elaboración propia de las autoras



Así mismo, en la etapa de preservación se pudo observar que no se considera la práctica de desconectar equipos detectados como evidencia conectados a una red y no designan a una persona como custodio de pruebas, con el propósito de fotografiar, documentar y etiquetar cada elemento que se recoge, y registrar cada acción que se realizó junto con quien realiza la acción, dónde fue realizado y en qué momento. Ver figura 11.

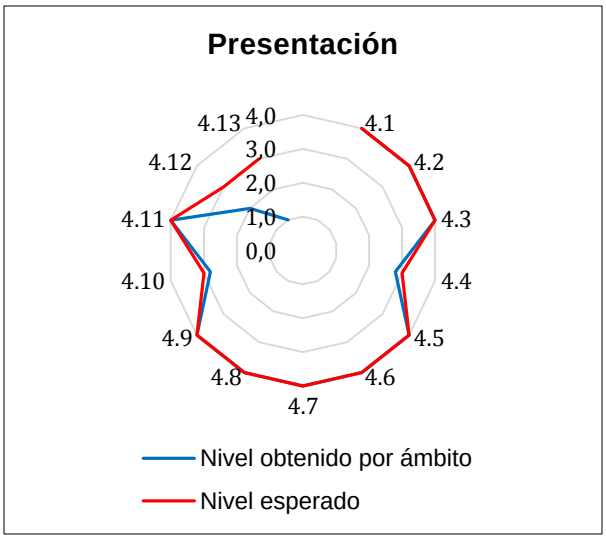
Figura 11: Nivel de madurez de la preservación
Fuente: Elaboración propia de las autoras

De la misma manera, en la fase de adquisición se determinó que no se considera ejecutar el levantamiento de los datos acorde al previo análisis de niveles de relevancia o prioridad, del tipo de dispositivo y del orden de volatilidad de la información, determinar lo más rápido posible si la volatilidad de los datos debe ser preservada, verificar si el dispositivo está accediendo a datos remotos, archivos

versidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
versidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

encriptados o con claves de acceso, correspondencia o comunicaciones electrónicas, datos de carácter personal entre otros. Así mismo, los peritos se basan en el formato del informe pericial, documentan la técnica usada en la pericia sin especificar a detalle lo correspondiente a la etapa de adquisición. Sin embargo, si desarrollan un plan de extracción de datos en donde se detallan las preguntas que se quieren responder respecto al caso, pero no consideran en el plan la priorización de las fuentes de datos, así como tampoco establecen el orden en que los datos van a ser adquiridos. Ver figura 12.

Figura 12: Nivel de madurez de la adquisición
Fuente: Elaboración propia de las autoras



Así mismo, en la fase de análisis la especificación de la hora de la BIOS del equipo informático en donde van instalados los discos duros que contienen la información de interés, la revisión de los encabezados de los archivos y la información a quien solicitó el peritaje si se encuentran nuevas evidencias del incidente solo se ejecutan de manera parcial.

Sin embargo, considerando la experiencia de cada perito si se ejecutan de manera independiente la revisión de los registros del sistema y de las aplicaciones que puedan estar presentes como registros de error, registros de instalación, conexión de registros, registros de seguridad entre otros, la revisión de los sellos de fechas y hora que figura en el sistema de archivos de metadatos para vincular archivos de interés, la examinación la estructura de partición del disco para determinar si todo el tamaño físico de la unidad de disco duro se contabiliza y el establecimiento del orden de prioridad de la prueba que se va a examinar. Ver figura 13.

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

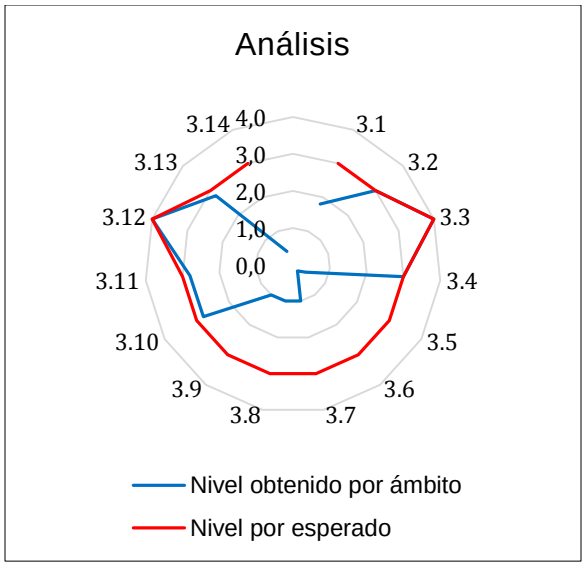


Figura 13: Niveles de madurez de análisis
Fuente: Elaboración propia de las autoras

Por otro lado, en la fase de presentación existen procesos maduros como el uso de una plantilla estándar que incluye el detalle de las técnicas utilizadas, la naturaleza de los hechos investigados, la ubicación donde ocurrió la incidencia, el objetivo de la investigación, los miembros del equipo de investigación junto a sus funciones, la duración de la investigación, la ubicación de la investigación y los detalles de las pruebas digitales que se han observado durante la investigación; sin embargo, el informe no incluye las recomendaciones para continuar con la investigación o trabajos futuros, ni las limitaciones del análisis realizado. Ver figura 14.
Figura 14: Nivel de madurez de presentación
Fuente: Elaboración propia de las autoras

Así mismo, en la etapa final que corresponde al manejo de expedientes se detectó que no se documenta las irregularidades y las medidas tomadas durante el examen, poseen únicamente lo documentado en el informe pericial. De igual manera, no se almacena a largo plazo la información confidencial capturada por herramientas forenses, que asegure que esto no infringe la privacidad de los involucrados; solo se guarda exclusivamente lo capturado para las evidencias incluidas en el informe pericial. Ver figura 15 y anexo C.

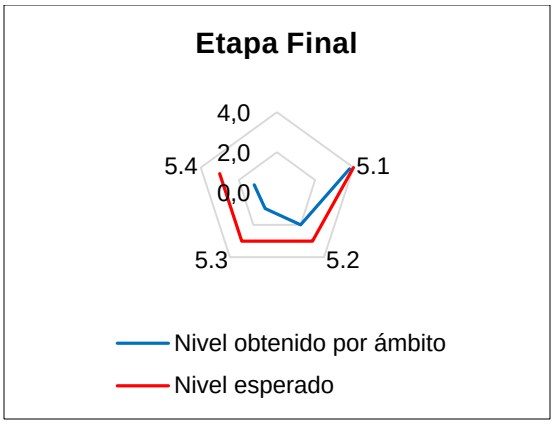


Figura 15: Nivel de madurez de la etapa final
Fuente: Elaboración propia de las autoras

CONCLUSIONES

En la presente investigación se ha realizado el análisis de brecha del proceso de computación forense en Ecuador respecto a las buenas prácticas internacionales, el cual ha permitido determinar que en la actualidad Ecuador está ubicado en el nivel dos de madurez.

Así mismo, se pudo conocer que de las seis etapas analizadas la de mayor nivel de madurez es la de presentación. De la misma manera, todas las etapas han alcanzado y superado el nivel de madurez dos, por lo que las oportunidades de mejora propuestas van orientadas a alcanzar un nivel de madurez 3 (estado deseado).

Es por ello, que los hallazgos más destacados muestran la necesidad de contar con un marco de trabajo que contenga protocolos de actuación tipificados que guíen el transcurso de la pericia informática apegada a un debido proceso.

Así mismo, se observa la importancia de capacitar de manera constante a los peritos calificados, en temas que refuercen sus actividades de peritaje informático, debido a que esto es transcendental a la hora de aplicar los procesos implementados.

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

De la misma manera, es prioritario estandarizar procesos que ya son aplicados en la actualidad en la pericia informática, mismos que deben ser socializados con todos los expertos y generar la documentación pertinente.

Por otro lado, dentro de las limitaciones en este estudio es posible resaltar la dificultad para acceder a la información, los análisis forenses ejecutados en Ecuador, a los informes de los casos procesales sentenciados, la limitada cantidad de peritos para el juicio de expertos y el tiempo requerido por parte de los expertos para obtener la información necesaria; por lo cual, fue posible incluir 10 informes de casos sentenciados y contar con el aporte de 5 peritos de diferentes ciudades.

Así pues, este estudio exploratorio al ser un tema que inicia en el país sirve de referente para futuras investigaciones como ejecutar el análisis de brechas por provincia, analizar del perfil idóneo del perito informático o analizar las herramientas que puedan soportar el proceso de pericia informática en Ecuador.

BIBLIOGRAFÍA

Al Fahdi, M., Clarke, N., Li, F., & Furnell, S. (2016). A suspect-oriented intelligent and automated computer. *Digital Investigation*, 65-76.

Alharbi, S., Weber, J., & Traore, I. (2011). The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review. *International Conference on Information Security and Assurance*, 87-100.

Amaya, H. (2012). Aspectos Técnicos Y Herramientas

Álvarez, A. F., Marín, O. D. M., & Victoria, J. D. V. (2012). Framework Para La Computación Forense En Colombia, *3*(2), 61–69.

Ariza, A., Ruíz, J., & Cano, J. (2009). iPhone 3G: Un Nuevo Reto para la Informática Forense. *Universidad Pontifica Javeriana, Bogotá-Colombia*, *1*(1), 1–15. Retrieved from https://www.researchgate.net/publication/228862122_iPhone_3G_Un_Nuevo_Reto_para_la_Informatica_Forense

Armilla, N., Panizzi, M., Eterovic, J., & Torres, L. (2017). Buenas prácticas para la recolección de la evidencia digital en la Argentina.

Ardita, J. (11 de 07 de 2007). Metodología de Análisis Forense Informático. Buenos Aires, Argentina.

Asociación de Tasadores y Peritos Judiciales Informáticos. (13 de 11 de 2017). *ANTPJI*. Obtenido de https://www.antpji.com/antpji2013/index.php/1156-aumentan-los-casos-en-los-juzgados-de-recusacion-del-perito-informatico-por-no-tener-la-capacitacion-adecuada

Asociación Española de Normalización y Certificación . (2013). Metodología para el análisis forense de las evidencias electrónicas. España.

Bartosz , I., & Lu, L. (2014). Enhanced Timeline Analysis for Digital Forensic. *Information Security Journal: A Global Perspective*, 32-34.

Builtrago, H. (2014). *Universidad Católica de Pereira.* Obtenido de http://repositorio.ucp.edu.co:8080/jspui/bitstream/10785/3653/1/CDMIST92.pdf

Bolaños, F. (2015). Estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador, (3).

Carrier, B., & Spafford, E. (2004). An event-based digital forensic investigation framework. Digital Forensic Research Workshop, 1–12. https://doi.org/10.1145/1667053.1667059

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

Cano, J. (2006). Introducción a la informática forense. *Sistemas*, 64-66.

Cano, J. (2006). *Universidad de los Andres.* Obtenido de http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/JeimyCano_VIJNSI.pdf

Cano, J . (2016). iPhone 3G : Un Nuevo Reto para la Informática Forense, (October).

Carroll , O., Brannon, S., & Song, T. (01 de 2008). *Department of Justice of United State.* Obtenido de https://www.justice.gov/sites/default/files/usao/legacy/2008/02/04/usab5601.pdf

Córdova, K. (28 de 11 de 2014). *Informática Forense*. Obtenido de http://informaticaforensekarolcordoba.blogspot.com/2014/11/historia-de-la-informatica-forense.html

Ćosić, J., Ćosić, Z., & Bača, M. (2011). An ontological approach to study and manage digital chain of custody of digital evidence. Journal of Information and Organizational Sciences, 35(1), 1–13.

Costantini, S., De Gasperis, G., & Olivieri, R. (2015). Digital Forensics Evidence Analysis: An Answer Set Programming Approach for Generating Investigation Hypotheses. *Research Gate*, 242-249.

Delgado, M. L. (2007). Análisis forense digital. *Hackers&Seguridad*, 3-5.

Di Iorio. (2016). LA INFORMÁTICA FORENSE Y EL PROCESO DE RECUPERACIÓN DE INFORMACIÓN DIGITAL, 326–339.

Escobar, J., & Cuervo, Á. (2008). Validez De Contenido Y Juicio De Expertos: Una Aproximación a Su Utilización. Avances En Medición, 6, 27–36.

Fernández, D. (05 de 2004). Recuperación de la Evidencia Digital. Barcelona, España.

Fuentes, T., & Ricaurte, B. (2015). Evidencia forense digital en equipos de cómputo, redes y Resumen Introducción, 9–24.

Garay, R., Espinoza, A., Martínez, A., & Castro, L. (2013). Estudio de Mapeo Sistematizado sobre la Estimación de Valor del Producto Software, (September 2014), 138–145. https://doi.org/10.13140/2.1.2987.9688

García Valdés, M., & Suárez Marín, M. (2013). El método Delphi para la consulta a expertos en la investigación científica Delphi method for the expert consultation

Guerra, C. D. G. (2014). ANALISIS Y APLICACIÓN DE SOFTWARE PARA LA RECUPERACIÓN FORENSE DE EVIDENCIA DIGITAL EN DISPOSITIVOS MÓVILES ANDROID.

ISACA. (2015). *ISACA.* Obtenido de http://isaca.org/Knowledge-Center/Research/Documents/Overview-of-Digital-Forensics_whp_Eng_0315.pdf

ISO/IEC. (2015). Guidelines for the analysis and interpretation of digital evidence.

Justicia, M. De. (2014). Código Orgánico Integral Penal

Lerena, R. G., Di Iorio, A., Podestá, A., & Constanzo, B. (2015). Informática Forense.

Locard. (2012). Obtenido de https://www.forensichandbook.com/locards-exchange-principle/

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

Lema, L. (2016). MODELO PARA LA TOMA DE DECISIONES MULTICRITERIO COMO SOPORTE PARA EL ANÁLISIS FORENSE EN DISPOSITIVOS DE ALMACENAMIENTO DIGITAL.

Montoya, A. (2010). LA INFORMÁTICA FORENSE COMO HERRAMIENTA PARA LA APLICACIÓN. Colombia.

NIST. (2016). National Institute of Standards and Technology.

Padilla, J. (2014). *Javier Padilla*. Obtenido de http://ing.javierpadilla.over-blog.es/2014/11/informatica-forense.html

Policía Científica de España. (06 de 2011). Cien años de Policía Científica. España.

Piccirilli. (2015). Universidad Nacional de La Plata Facultad de Informática TESIS Doctoral en Ciencias Informáticas PROTOCOLOS A APLICAR EN LA FORENSIA DE LAS NUEVAS TECNOLOGÍAS (PERICIA – FORENSIA y CIBERCRIMEN)."

Real Academia Española. (2010). *Real Academia Española*. Obtenido de http://dle.rae.es/srv/search?m=30&w=metodolog%C3%ADa

Rodriguez , F., & Doménech, A. (20 de 08 de 2011). Obtenido de https://cj-worldnews.com/spain/index.php/es/criminalistica-29/item/1786-la-inform%C3%A1tica-forense-el-rastro-digital-del-crimen

Rojas, F. (2017). Novedades sobre la informática forense en México y Latinoamérica. *TEMA Revisa Digital de Criminología y Seguridad*, 44-58.

Roatta, S., Casco, M. E., & Fogliato, M. (2012). El tratamiento de la evidencia digital y las normas ISO / IEC 27037:2012.

Schultz, E. (2007). Computer forensics challenges. *IDS Forensic*, 12-15.

Santos, L. M., & Flórez, A. S. (2013). Metodología Para El Análisis Forense En Linux. *Revista Colombiana De Tecnologias De Avanzada (Rcta)*, *2*(20). https://doi.org/10.24054/16927257.V20.N20.2012.194

The Hill. (02 de 11 de 2017). Obtenido de http://thehill.com/policy/cybersecurity/358511-trump-signs-cyber-crime-bill

Vera, E. (6 de 07 de 2017). *Detectives Madrid*. Obtenido de http://www.detectives-madrid.es/historia-informatica-forense-aplicacion/

Villamil, C. (23 de 12 de 2014). *Seguridad Informática*. Obtenido de http://seginformaticacarolinavillamil.blogspot.com/p/el-campo-de-la-informatica-forense-se.html

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

ANEXOS

ANEXO A: SELECCIÓN DE METODOLOGÍAS A ANALIZAR

Significado	
Si	1
No	0

Computación forense ejecutada en Ecuador	METODOLOGÍAS DE COMPUTACIÓN FORENSE						
	Departamento de Justicia de Estados Unidos	Instituto Nacional de Estándares y Tecnologías	EC-COUNSIL	Guía Integral Argentina	Red Europea de Institutos Forenses	UNE 71506:2013	ISO/IEC 27042:2015
Fase: Preparación	1	0	0	0	1	0	0
Fase: Identificación	1	1	0	1	1	1	1
Fase: Análisis	1	1	1	1	1	1	1
Fase: Documentación	1	1	1	1	1	1	1
Recibir una orden fiscal	1	1	1	1	1	0	0
Determinar el alcance y objeto de la pericia	1	0	0	1	1	1	1
Autorización para ingresar a correos, archivos o equipos en general.	0	0	0	1	0	0	0
Imagen forense de la evidencia a analizar	1	1	1	1	1	1	1
Creación de códigos hash	1	1	1	1	1	1	1
Ubicar sellos de seguridad y etiquetado a las evidencias	0	0	0	0	1	1	0
Evidencias fotográficas de cómo se recibe el equipo	1	1	0	1	1	1	1
Presentación física y digital de las fotografías	1	1	0	1	1	1	1

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

tomadas							
Registro de las características de la evidencia	1	1	1	1	1	1	1
Uso de formatos documentales	1	1	1	1	1	1	1
Uso de medios magnéticos para el almacenamiento de la evidencia digital	0	0	0	1	1	1	1
Utilización de software libre y de pago para el análisis de la evidencia	1	1	0	1	1	1	1

Consolidado	
Metodologías	**Número de actividades cumplidas**
Departamento de Justicia de Estados Unidos	13
Instituto Nacional de Estándares y Tecnologías	11
EC-COUNSIL	7
Guía Integral Argentina	14
Red Europea de Institutos Forenses	15
UNE 71506:2013	13
ISO/IEC 27042:2015	12

ANEXO B: CALCULO DEL NIVEL DE MADUREZ DEL ANÁLISIS DE BRECHAS

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

Guía de Evaluación (Escala)	
0	El proceso no existe
1	El proceso está establecido
2	El proceso está implementado
3	El proceso es mantenido y existen documentos.
4	El proceso está en mejora continua

Etapa inicial	Actividades	Nivel de madurez					Intervalos	Nivel obtenido	Nivel esperado
		0	1	2	3	4			
0.1	Conocer las políticas de seguridad que posee la organización en aspectos como control de acceso a las máquinas y dispositivos, existencia o no de un registro de eventos, conocimiento de un plan de auditorías periódicas, conocimiento del sistema de gestión o control de las copias de los datos.	0	0	5	0	0	5	2,0	3,0
0.2	Revisar los procesos y prácticas de análisis forenses actuales y en base a ello, identificar las deficiencias de la normativa, errores de procedimiento y otras cuestiones que deben ser subsanadas, manteniendo la tendencia de la tecnología y los cambios de ley.	1	3	1	0	0	5	1,0	3,0
0.3	Determinar qué proceso legal adicional puede ser necesario continuar la búsqueda si llegase a encontrar una evidencia que no estaba autorizada en la orden fiscal	0	1	4	0	0	5	1,8	3,0
0.4	Supervisar la cadena de custodia previa hasta la llegada de las evidencias al entorno de análisis forense	0	5	0	0	0	5	1,0	3,0
0.5	Preparar un plan de investigación documentada que ayude a la determinación de los recursos, la selección de los procesos y herramientas para orientar al equipo de investigación	0	0	5	0	0	5	2,0	3,0
0.6	Realizar una labor previa de localización de las evidencias que confirme la existencia de un incidente y las causas que lo	2	0	1	2	0	5	1,6	3,0

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

	originaron								
0.7	Actualizar periódicamente a los examinadores forenses con las últimas herramientas y técnicas que abordan las últimas tecnologías.	0	0	2	3	0	5	2,6	3,0
0.8	Evaluar el nivel de destreza de los usuarios informáticos involucrados	0	0	4	0	1	5	2,4	3,0
0.9	Determinar que tipos de datos se recogen mejor por los funcionarios encargados de hacer cumplir la ley.	0	4	0	1	0	5	1,4	3,0
0.10	Validar y confirmar los procesos que implican el uso de nuevos instrumentos antes de la implementación.	0	2	0	3	0	5	2,2	3,0
0.11	Tener un kit de herramientas forenses para la recolección de datos, examen y análisis	0	1	0	4	0	5	2,6	3,0
0.12	Conocer el objetivo, alcance y destinatarios que tendrá la investigación	0	0	0	0	5	5	4,0	4,0
0.13	Comprobar que el objeto y alcance de lo que se precisa estudiar está dentro de la competencia del entorno forense	0	0	1	4	0	5	2,8	3,0
0.14	Incluir un documento de recepción y registro de la evidencia recibida	0	0	0	0	5	5	4,0	4,0
0.15	Redactar el detalle de las informaciones recibidas y las decisiones que se toman, incluidos los motivos de la decisión.	0	0	1	4	0	5	2,8	3,0
0.16	Ejecutar el proceso de análisis forense mediante un proceso consistente.	0	0	0	5	0	5	3,0	3,0
0.17	Poseer protocolos detallados que aseguren la integridad de las evidencias objeto del estudio forense	0	0	3	2	0	5	2,4	3,0
0.18	Asegurar la independencia de las actuaciones forenses, preferible con un fedatario público que de fe del proceso	2	3	0	0	0	5	0,6	3,0
0.19	Verificar el funcionamiento del sistema informático del examinador que incluye hardware y software	0	1	1	3	0	5	2,4	3,0
0.20	Contar con un esquema de codificación de los casos investigados o en investigación que refleje su identificación, fecha d e incio y finalización, orden de legada, estado entre otros.	0	3	2	0	0	5	1,4	3,0
0.21	Contar con conjuntos separados	0	0	5	0	0	5	2,0	3,0

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

	formal y técnicamente de equipos e infraestructura para la parte administrativa y para la parte de laboratorios de investigación forense.								
NIVEL DE LA ETAPA INICIAL								2,2	3,1

Ambito 1: Preservación	Actividades	Nivel de madurez					Intervalos	Nivel obtenido	Nivel esperado
		0	1	2	3	4			
1.1	Impedir el acceso no autorizado y a la alteración de las pruebas.	1	0	0	3	1	5	2,6	3,0
1.2	Designar a una persona como custodio de pruebas, donde tenga la responsabilidad exclusiva de fotografiar, documentar y etiquetar cada elemento que se recoge, y registrar cada acción que se realizó junto con quien realiza la acción, dónde fue realizado y en qué momento	1	0	4	0	0	5	1,6	3,0
1.3	Fotografiar y grabar en video la escena de interés	0	0	0	0	5	5	4,0	4,0
1.4	Manipular las evidencias con la indumentaria adecuada, especialmente adaptada para evitar descargas electrostáticas.	0	0	0	5	0	5	3,0	3,0
1.5	Efectuar un estudio del área física y reconocer las posibles fuentes de datos.	0	0	0	4	1	5	3,2	3,2
1.6	Determinar el número y tipo de equipos en la escena	0	0	0	4	1	5	3,2	3,2
1.7	Documentar la ubicación desde el cual los medios fueron retirados.	0	0	0	5	0	5	3,0	3,0
1.8	Aislar los sistemas pertinentes de influencias externas para prevenir mayores daños al sistema.	0	0	0	4	1	5	3,2	3,2
1.9	Documentar los detalles de cada una de las pruebas encontradas antes y durante el proceso de análisis forense	0	1	4	0	0	5	1,8	3,0
1.10	Crear una lista de todos los usuarios que tienen acceso a los equipos que están siendo analizados para que puedan	0	0	5	0	0	5	2,0	3,2

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

	proporcionar sobre el lugar de alguna información importante.								
1.11	Evaluar la necesidad de proporcionar alimentación eléctrica continua para aparatos que funcionan con pilas.	0	0	5	0	0	5	2,0	3,0
1.12	Si el equipo detectado como evidencia está conectado a una red se deben desconectar los cables.	0	5	0	0	0	5	1,0	3,0
1.13	Utilizar fuentes de datos alternativas si no es posible recopilar datos de una fuente primaria.	0	0	3	2	0	5	2,4	3,0
1.14	Almacenar la evidencia digital en soportes adecuados antes y durante el análisis para garantizar la integridad.	0	0	0	4	1	5	3,2	3,2
1.15	Sellar en soportes adecuados todas las evidencias encontradas, hasta que se active su análisis por los peritos dentro del laboratorio de análisis forense para garantizar la integridad.	1	0	0	4	0	5	2,4	3,0
NIVEL DEL AMBITO 1: PRESERVACIÓN								2,6	3,1

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

Ambito 2: Adquisición	Actividades	Nivel de madurez					Intervalos	Nivel obtenido	Nivel esperado
		0	1	2	3	4			
2.1	Crear un plan que priorice las fuentes de datos	0	4	1	0	0	5	1,2	3,0
2.2	Establecer el orden en que los datos van a ser adquiridos	0	5	0	0	0	5	1,0	3,0
2.3	Documentar cada paso ejecutado en la adquisición de los datos	0	4	1	0	0	5	1,2	3,0
2.4	Determinar los posibles tipos de pruebas que se persiguen	0	0	4	1	0	5	2,2	3,0
2.5	Adoptar los principios de la cadena de custodia al soporte de la información adquirida, acompañada de la obtención de un código hash para posterior validación.	1	0	0	0	4	5	3,2	4,0
2.6	Crear un acta de levantamiento de evidencia digital	0	0	3	2	0	5	2,4	3,0
2.7	Localizar todos los equipos inalámbricos determinando todos los modos de comunicación que usan éstos	0	1	3	1	0	5	2,0	3,0
2.8	Documentar el estado del dispositivo como marca, modelo, tamaño, configuración, ubicación, MAC, tarjeta de red entre otros que se consideren fundamentales.	0	0	0	0	5	5	4,0	4,0
2.9	Fotografiar y etiquetar las pruebas para proporcionar recordatorios visuales de la configuración del equipos y periféricos.	0	0	1	3	1	5	3,0	3,0
2.10	Desconectar los dispositivos de almacenamiento para evitar la destrucción, deterioro o alteración de los datos.	0	1	3	1	0	5	2,0	3,0
2.11	Si se detecta que el dispositivo está accediendo a datos remotos, archivos encriptados o con claves de acceso, correspondencia o comunicaciones electrónicas, datos de carácter personal entre otros se debe consultar al responsable del procedimiento acerca de los límites que pudieran existir	0	4	1	0	0	5	1,2	3,0

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

	para la captura de la información.								
2.12	Buscar en dicho entorno todo tipo de notas asociadas a las palabras de paso y al PIN de acceso a los equipos	0	3	2	0	0	5	1,4	3,0
2.13	Hacer uso de herramientas de adquisición de datos confiables	0	0	0	4	1	5	3,2	4,0
2.14	Activar la protección contra escritura para preservar y proteger la evidencia original.	0	0	0	0	5	5	4,0	4,0
2.15	Estimar el valor probable relativo de cada fuente potencial de datos	0	1	3	1	0	5	2,0	3,0
2.16	Determinar lo más rápido posible si la volatidad de los datos debe ser preservada.	3	2	0	0	0	5	0,4	3,0
2.17	Seguir un procedimiento de adquisición documentado y utilizar herramientas de hardware y software reconocidas en el ámbito forense	0	0	5	0	0	5	2,0	3,0
2.18	De forma previa el disco duro usado para guardar el clonado forense debe ser sometido a un borrado seguro y estar dentro de su vida útil	0	0	1	4	0	5	2,8	3,0
2.19	Realizar dos resúmenes digitales (hash) de la información contenida en el disco duro de forma simultánea al proceso de clonado, usando herramientas de hardware o software contrastadas en el ámbito forense y verificar que ambos resúmenes sean los mismos.	1	0	0	4	0	5	2,4	3,0
2.20	Procurar la menor alteración y /o destrucción de datos informáticos; de darse el caso debe precisar en forma documentada en que ha consistido la alteración y cuáles son los efectos sobre el material probatorio adquirido.	0	0	1	3	1	5	3,0	3,0
2.21	Realizar una copia maestra y una copia de trabajo, y trabajar sobre la copia maestra.	0	0	5	0	0	5	2,0	3,0

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

2.22	Ejecutar el levantamiento de los datos acorde al previo análisis de niveles de relevancia o prioridad, del tipo de dispositivo y del orden de volatilidad de la información.	3	2	0	0	0	5	0,4	3,0
2.23	Verificar la integridad de los datos adquiridos	0	0	1	3	1	5	3,0	3,0
2.24	Discutir si otros procesos forenses tienen que llevarse a cabo sobre la evidencia	0	0	3	1	1	5	2,6	3,0
2.25	Analizar la posibilidad de emprender otras vías de investigación para obtener más pruebas digitales	0	0	1	4	0	5	2,8	3,0
2.26	Determinar información adicional que puede ayudar a resolver el caso	0	0	0	4	1	5	3,2	4,0
NIVEL DEL AMBITO 2: ADQUISICIÓN								2,3	3,2

Ámbito 3: Análisis	**Actividades**	**Nivel de madurez**					**Intervalos**	**Nivel obtenido**	**Nivel por esperado**
		0	**1**	**2**	**3**	**4**			
3.1	Establecer el orden de prioridad de la prueba que se va a examinar	0	1	4	0	0	5	1,8	3,0
3.2	Mantener notas contemporáneas detalladas y precias de las cada actuación ejecutada y los procesos que estas demandaron.	0	0	0	5	0	5	3,0	3,0
3.3	Comprobar que las evidencias no están deterioradas y son susceptibles de su estudio forense	0	0	0	0	5	5	4,0	4,0
3.4	Identificar los tipos de archivos desconocidos para determinar su valor en la investigación	0	0	0	5	0	5	3,0	3,0
3.5	Revisar los encabezados de los archivos	3	2	0	0	0	5	0,4	3,0
3.6	Especificar la hora de la BIOS del equipo informático en donde van instalados los discos duros que contienen la información de interés	4	1	0	0	0	5	0,2	3,0
3.7	Revisar los registros del sistema y de las aplicaciones que puedan estar presentes como registros de error, registros de instalación, conexión de registros, registros	0	5	0	0	0	5	1,0	3,0

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

	de seguridad entre otros.								
3.8	Revisar los sellos de fechas y hora que figura en el sistema de archivos de metadatos para vincular archivos de interés.	0	5	0	0	0	5	1,0	3,0
3.9	Examinar la estructura de partición del disco para determinar si todo el tamaño físico de la unidad de disco duro se contabiliza.	0	5	0	0	0	5	1,0	3,0
3.10	Revisar nombres de archivos relevantes y patrones	0	0	1	4	0	5	2,8	3,0
3.11	Examinar las relaciones entre archivos	0	0	1	4	0	5	2,8	3,0
3.12	Estudiar la documentación adjunta a las evidencias	0	0	0	0	5	5	4,0	4,0
3.13	Considerar nuevas evidencias relevantes en el proceso que no habían sido contempladas en un principio, iniciando nuevamente la reseña de éstas, generando un nuevo proceso de gestión, custodia y trazabilidad.	0	0	1	4	0	5	2,8	3,0
3.14	Informar a quien solicitó el peritaje si se encuentra nuevas evidencias del incidente y esperar por nuevas instrucciones	3	2	0	0	0	5	0,4	3,0
NIVEL DEL AMBITO 3: ANÁLISIS								2,0	3,1

Ambito 4: Presentación	**Actividades**	**Nivel de madurez**					**Intervalos**	**Nivel obtenido por ámbito**	**Nivel esperado**
		0	**1**	**2**	**3**	**4**			
4.1	Ubicar la identidad de la agencia/departamento/unidad y perito(s) que ejecutaron el análisis forense.	0	0	0	0	5	5	4,0	4,0
4.2	Ubicar el número identificador del caso, la fecha de recepción del caso y la fecha del informe	0	0	0	0	5	5	4,0	4,0
4.3	Incluir la naturaleza de los hechos investigados, la ubicación donde ocurrió la incidencia, el objetivo de la investigación, los miembros del equipo de investigación junto a sus funciones, la duración de la investigación, la ubicación de la	0	0	0	0	5	5	4,0	4,0

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

	investigación, los detalles de las pruebas digitales que se han observado durante la investigación.								
4.4	Incluir una declaración clara del escritor que participó en la investigación.	0	0	1	4	0	5	2,8	3,0
4.5	Usar una plantilla de informe con formato estandarizado para ayudar a garantizar que existe suficiente información incluida en los mismos.	0	0	0	0	5	5	4,0	4,0
4.6	Detallar la información general de los dispositivos analizados, tales como marca, modelo, número de serie entre otros.	0	0	0	0	5	5	4,0	4,0
4.7	Describir brevemente las medidas adoptadas durante el examen, tales como búsquedas de cadenas, búsquedas de imágenes, gráficos y recuperar archivos borrados	0	0	0	0	5	5	4,0	4,0
4.8	Describir los programas utilizados en el análisis de la evidencia	0	0	0	0	5	5	4,0	4,0
4.9	Detallar las técnicas utilizadas	0	0	0	0	5	5	4,0	4,0
4.10	Informar si las pruebas digitales han tenido cualquier daño	0	0	1	4	0	5	2,8	3,0
4.11	Determinar los resultados y conclusiones del caso.	0	0	0	0	5	5	4,0	4,0
4.12	Incluir las limitaciones de cualquier análisis realizado	0	0	5	0	0	5	2,0	3,0
4.13	Incluir las recomendaciones para continuar con la investigación o trabajos futuros.	0	5	0	0	0	5	1,0	3,0
NIVEL DEL AMBITO 4: PRESENTACIÓN								3,4	3,7

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

Etapa final: Manejo de expedientes	Actividades	Nivel de madurez					Intervalos	Nivel obtenido	Nivel esperado
		0	1	2	3	4			
5.1	Mantener una copia de la orden judicial emitida por el fiscal o juez con el expediente del caso.	0	0	0	1	4	5	3,8	4,0
5.2	Mantener una copia de la cadena de custodia	0	0	5	0	0	5	2,0	3,0
5.3	Documentar las irregularidades y las medidas tomadas durante el examen	0	5	0	0	0	5	1,0	3,0
5.4	Almacenar a largo plazo la información confidencial capturada por herramientas forenses, asegurándose que esto no infringe la privacidad de los involucrados.	0	4	1	0	0	5	1,2	3,0
NIVEL DE LA ETAPA FINAL: MANEJO DE EXPEDIENTES								2,0	3,3

Ámbitos	Nivel obtenido	Nivel esperado
Etapa previa	2,2	3,0
Ámbito 1: Preservación	2,6	3,0
Ámbito 2: Adquisición	2,3	3,0
Ámbito 3: Análisis	2,0	3,1
Ámbito 4: Presentación	3,4	3,7
Etapa final	2,0	3,3
Nivel de Madurez General	2,4	3,2

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

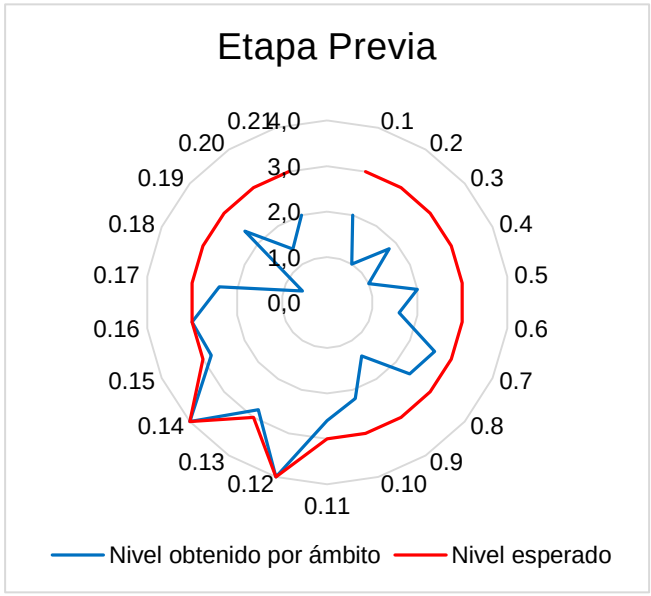
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

ANEXO C: RESUMEN DE LOS RESULTADOS OBTENIDOS

ETAPA PREVIA

Componentes evaluados

- Conocimiento de las políticas de seguridad de la organización
- Revisión de procesos y prácticas de análisis forenses actuales
- Determinación de procesos legales adicionales
- Conocimiento de la cadena de custodia
- Plan de investigación documentada
- Confirmación de la existencia del incidente
- Actualización de los examinadores forenses
- Evaluar el nivel de destreza de los usuarios informáticos involucrados
- Validación y confirmación de procesos que implican el uso de nuevos instrumentos antes de la implementación.
- Tener un kit de herramientas forenses para la recolección de datos, examen y análisis
- Conocimiento del objetivo, alcance y destinatarios de la investigación
- Entrega y recepción de la evidencia recibida
- Proceso de análisis forense y existencia de protocolos detallados
- Independencia de las actuaciones forenses
- Existencia de un esquema de codificación de casos investigados o en investigación
- Equipos e infraestructura



ob	Hallazgos Relevantes	Nivel de madurez Actual	Nivel de madurez Esperado

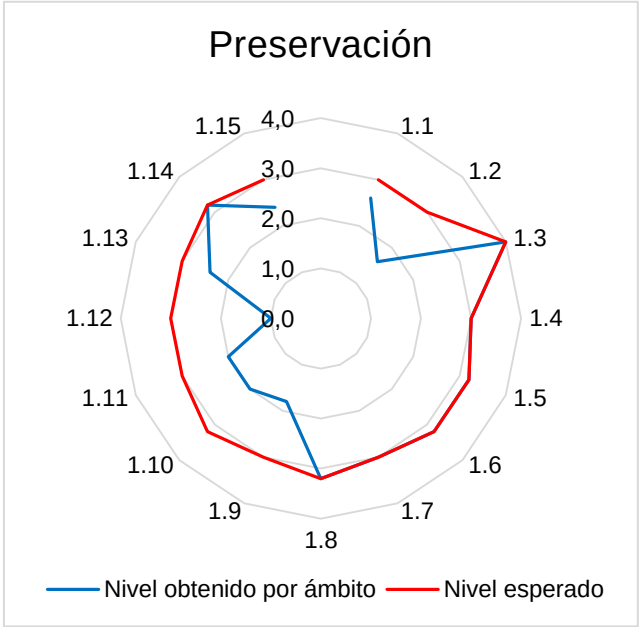
[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

	Conocimiento de las políticas de seguridad de la organización: • No siempre se conoce las políticas de seguridad, registro de eventos, plan de auditorías, conocimiento del control de copia de datos; lo habitual es conocer el control de acceso a las máquinas y dispositivos **Revisión de procesos y prácticas de análisis forenses actuales:** • Los peritos se limitan a seguir y cumplir el procedimiento estipulado en el Reglamento del sistema pericial integral de la función judicial, no existe feedback, no se identifica las deficiencias de la normativa, errores de procedimiento y otras cuestiones que deben ser subsanadas, manteniendo la tendencia de la tecnología y los cambios de ley. **Determinación de procesos legales adicionales:** • No es una práctica común para algunos peritos determinar si existe un elemento incriminatorio que esté fuera de la orden judicial, se limitan a investigar lo que en la orden se solicita. **Conocimiento de la cadena de custodia:** • La cadena de custodia no es supervisada desde el estado previo hasta la llegada de las evidencias al entorno de análisis forense, la hoja de registro es enviada para ser firmada solo a las personas que manipulan la evidencia. **Plan de investigación documentada:** • Los expertos no elaboran un plan de investigación documentada que ayude a la determinación de los recursos, la selección de los procesos y herramientas para orientar al equipo de investigación; los peritos desarrollan un plan de extracción de datos para realizar la investigación, pero no existe un documento formal que tipifique el proceso. **Confirmación de la existencia del incidente:** • No se ejecuta una labor previa de localización de las evidencias que confirme la existencia de un incidente y las causas que lo originaron, los expertos localizan solo los dispositivos a analizar en la escena del crimen **Actualización periódica de los examinadores forenses:** • La mayoría de los peritos no recibe actualización en temas relacionados a peritaje informático con las últimas herramientas y técnicas que abordan las últimas tecnologías.			Oportunidades de mejora	• Generar documentación de un proceso con protocolos específicos tipificados para la actuación en la pericia informática. • Incluir en el proceso previo el conocimiento de acciones ejecutadas en la organización objeto de estudio como las políticas de seguridad, registro de eventos, plan de auditorías, control de copia de datos • Identificar deficiencias de las normativas y errores de procedimiento para proponer su debido proceso. • Determinar la existencia de elementos incriminatorios que estén fuera de la orden fiscal. • Supervisar de la cadena de custodia previa y en el proceso. • Documentar el plan de extracción de datos • Realizar la confirmación de la existencia del incidente. • Capacitar de manera constante a los peritos calificados, en temas que refuercen sus actividades de peritaje informático. • Normalizar y documentar el proceso que permite validar y confirmar el uso de nuevos
	Evaluar el nivel de destreza de los usuarios informáticos involucrados • La mayoría de peritos no tienen formación para ejecutar el proceso, hace falta capacitación **Validación y confirmación de procesos que implican el uso de nuevos instrumentos antes de la implementación.** • Los equipos se validan antes de usarlos, se trata de un proceso que no se encuentra regulado en un documento **Tener un kit de herramientas forenses para la**				

estrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmm uees.edu.ec
estrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail: vber es@uees.edu.ec

PRESERVACION

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

<table>
<tr><td>Componentes evaluados</td><td colspan="3">Acceso no autorizado y alteración de las pruebas
Designación de una persona como custodio de pruebas
Fotos y grabación en video de la escena de interés
Manipulación de las evidencias con la indumentaria adecuada, especialmente adaptada para evitar descargas electrostáticas.
Estudio del área física y reconocimiento de las posibles fuentes de datos.
Determinación del número y tipo de equipos en la escena
Documentación de la ubicación desde el cual los medios fueron retirados.
Aislamiento de los sistemas pertinentes, de influencias externas para prevenir mayores daños al sistema.
Documentación de los detalles de cada una de las pruebas encontradas antes y durante el proceso de análisis forense
Existencia de una lista de todos los usuarios que tienen acceso a los equipos que están siendo analizados con el fin de proporcionar alguna información importante sobre el lugar.
Evaluación de la necesidad de proporcionar alimentación eléctrica continúa para aparatos que funcionan con pilas.
Equipos detectados como evidencia conectados a una red deben ser desconectados.
Uso de las fuentes de datos alternativas en caso de no ser posible recopilar datos de una fuente primaria.
Almacenamiento de la evidencia digital en soportes adecuados antes y durante el análisis para garantizar la integridad.
Sellado en soportes adecuados todas las evidencias encontradas, hasta que se active su análisis por los peritos dentro del laboratorio de análisis forense para garantizar la integridad.</td><td rowspan="2"> 
</td></tr>
<tr><td>ción obse rvad</td><td>Hallazgos Relevantes</td><td>Nivel de madurez Actual</td><td>Nivel de madurez Esperado</td></tr>
</table>

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

	Acceso no autorizado y alteración de las pruebas • La mayoría de los peritos aseguran la escena del delito físicamente para evitar accesos no autorizados y alteración de la evidencia **Designación de una persona como custodio de pruebas** • El proceso se encuentra implementado, aunque no es de conocimiento de todos los peritos **Fotos y grabación en video de la escena de interés** • Los expertos fotografían detalladamente cada evidencia **Manipulación de las evidencias con la indumentaria adecuada, especialmente adaptada para evitar descargas electrostáticas.** • Existe una manipulación adecuada con la indumentaria adecuada, aunque es necesario documentar el proceso. **Estudio del área física y reconocimiento de las posibles fuentes de datos.** **Determinación del número y tipo de equipos en la escena** • En éstos dos procesos la práctica común de los peritos es localizar los dispositivos a analizar en la escena del crimen; habilidad que debería ser socializada entre todos los expertos y documentada **Documentación de la ubicación desde el cual los medios fueron retirados.** • Los peritos manifiestan que se realiza el registro del análisis y hallazgos del caso en el informe pericial, como parte de los elementos solicitados en dicho informe **Aislamiento de los sistemas pertinentes, de influencias externas para prevenir mayores daños al sistema.** • Se tiene como práctica no encender o apagar los equipos a analizarse mientras no se tenga definido el tipo de adquisición a efectuarse. **Documentación de los detalles de cada una de las pruebas encontradas antes y durante el proceso de análisis forense.** • En la pericia realizada se acostumbra documentar todos los hallazgos y procedimientos en cada una de las etapas del peritaje. **Existencia de una lista de todos los usuarios que tienen acceso a los equipos que están siendo analizados con el fin de proporcionar alguna información importante sobre el lugar.** • La técnica usada incluye crear una lista de las personas con acceso a los equipos del laboratorio forense **Evaluación de la necesidad de proporcionar alimentación eléctrica contínua para aparatos que funcionan con pilas.** • El proceso existe pero no es conocido por todos los peritos **Equipos detectados como evidencia conectados a una**	2.6	3	Oportunidades de mejora	• Estandarizar protocolos de actuación, socializar con los peritos y generar la documentación de los procesos relacionados con: **1.** Impedir el acceso no autorizado y a la alteración de pruebas, **2.** Designar a una persona como custodio de pruebas, donde tenga la responsabilidad exclusiva de fotografiar, documentar y etiquetar cada elemento que se recoge, y registrar cada acción que se realizó junto con quien realiza la acción, dónde fue realizado y en qué momento. **3.** creación de una lista de todos los usuarios que tienen acceso a los equipos que están siendo analizados, **4**. evaluación de la necesidad de proporcionar alimentación eléctrica continua para aparatos que funcionan con pilas, **5.** Si el equipo detectado como evidencia está conectado a una red se deben desconectar los cables. • Documentar los procesos para que se manipule las evidencias con la indumentaria adecuada, especialmente adaptada para evitar descargas electrostáticas; y por otro al utilizar fuentes de datos alternativas si no es posible recopilar datos de una fuente primaria. • Considerar en la etapa de preservación si el equipo detectado como evidencia está conectado a una red se deben desconectar los cables. • Realizar una descripción estándar y a detalle del proceso seleccionado para la pericia ya que actualmente se lo hace únicamente de manera general.

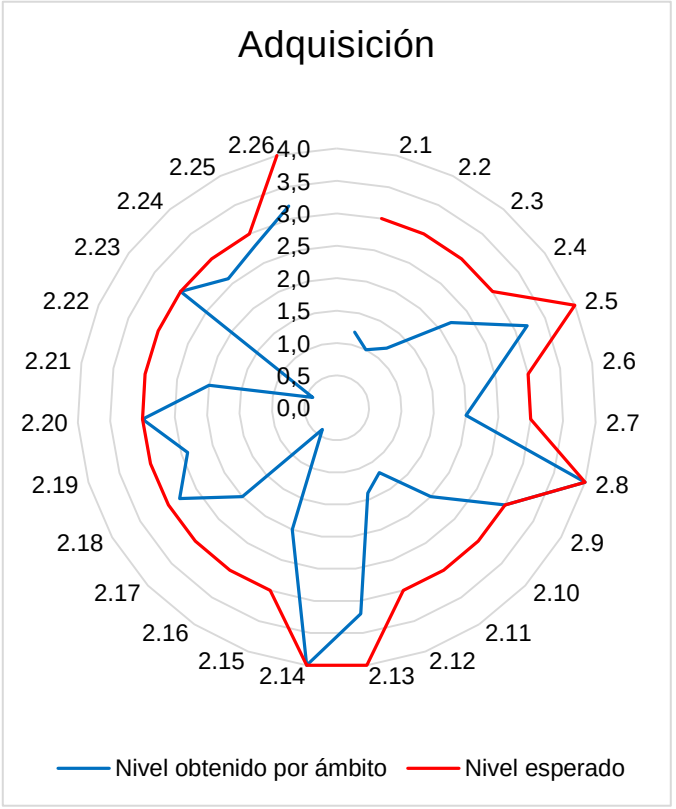
Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@u
Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides .ec

ADQUISICIÓN

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

Componentes evaluados

- Crear un plan que priorice las fuentes de datos y establecer el orden en que los datos van a ser adquiridos
- Documentar cada paso ejecutado en la adquisición de los datos
- Determinar los posibles tipos de pruebas que se persiguen
- Adoptar los principios de la cadena de custodia al soporte de la información adquirida, acompañada de la obtención de un código hash para posterior validación.
- Crear un acta de levantamiento de evidencia digital
- Localizar todos los equipos inalámbricos determinando todos los modos de comunicación que usan éstos
- Documentar el estado del dispositivo como marca, modelo, tamaño, configuración, ubicación, MAC, tarjeta de red entre otros que se consideren fundamentales.
- Fotografiar y etiquetar las pruebas para proporcionar recordatorios visuales de la configuración de los equipos y periféricos.
- Desconectar los dispositivos de almacenamiento para evitar la destrucción, deterioro o alteración de los datos.
- Si se detecta que el dispositivo está accediendo a datos remotos, archivos encriptados o con claves de acceso, correspondencia o comunicaciones electrónicas, datos de carácter personal entre otros se debe consultar al responsable del procedimiento acerca de los límites que pudieran existir para la captura de la información.
- Buscar en dicho entorno todo tipo de notas asociadas a las palabras de paso y al PIN de acceso a los equipos
- Hacer uso de herramientas de adquisición de datos confiables
- Activar la protección contra escritura para preservar y proteger la evidencia original.
- Estimar el valor probable relativo de cada fuente potencial de datos
- Determinar lo más rápido posible si la volatilidad de los datos debe ser preservada.
- Seguir un procedimiento de adquisición documentado y utilizar herramientas de hardware y software reconocidas en el ámbito forense
- De forma previa el disco duro usado para guardar el clonado forense debe ser sometido a un borrado seguro y estar dentro de su vida útil
- Realizar dos resúmenes digitales (hash) de la información contenida en el disco duro de forma simultánea al proceso de clonado, usando herramientas de hardware o software contrastadas en el ámbito forense y verificar que ambos resúmenes sean los mismos.
- Procurar la menor alteración y /o destrucción de datos informáticos; de darse el caso debe precisar en forma documentada en que ha consistido la alteración y cuáles son los efectos sobre el material probatorio adquirido.
- Realizar una copia maestra y una copia de trabajo, y trabajar sobre la copia maestra.
- Ejecutar el levantamiento de los datos acorde al previo análisis de niveles de relevancia o prioridad, del tipo de dispositivo y del orden de volatilidad de la información.
- Verificar la integridad de los datos adquiridos
- Discutir si otros procesos forenses tienen que llevarse a cabo sobre la evidencia
- Analizar la posibilidad de emprender otras vías de investigación para obtener más pruebas digitales
- Determinar información adicional que puede ayudar a resolver el caso



[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

ón observ	Hallazgos Relevantes	Nivel de madurez Actual	Nivel de madurez Esperado	

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

Crear un plan que priorice las fuentes de datos y establecer el orden en que los datos van a ser adquiridos

- La tarea ejecutada en ésta etapa es desarrollar un plan de extracción de datos en donde se detallan las preguntas que se quieren responder respecto al caso

Documentar cada paso ejecutado en la adquisición de los datos

- El proceso se encuentra establecido, aunque no es de conocimiento general, más todos los expertos se rigen en el formato del informe pericial solicitado sin especificar a detalle lo que correspondiente a la etapa de adquisición.

Determinar los posibles tipos de pruebas que se persiguen

- El proceso se encuentra implementado, los expertos revelan escoger el tipo de pruebas a ejecutar pero no existe documentación que respalde lo actuado.

Adoptar los principios de la cadena de custodia al soporte de la información adquirida, acompañada de la obtención de un código hash para posterior validación.

- El proceso se encuentra implementado de la siguiente manera: se crea resúmenes hash que permitan comprobar la integridad de la evidencia

Crear un acta de levantamiento de evidencia digital

Localizar todos los equipos inalámbricos determinando todos los modos de comunicación que usan éstos

- El proceso en ambas actividades es realizado por algunos expertos pero no es algo formal

Documentar el estado del dispositivo como marca, modelo, tamaño, configuración, ubicación, MAC, tarjeta de red entre otros que se consideren fundamentales.

- El proceso existe y esta implementado de manera adecuada

Fotografiar y etiquetar las pruebas para proporcionar recordatorios visuales de la configuración de los equipos y periféricos.

- El proceso se realiza en cierta medida con la información obtenida de cada análisis realizado

Desconectar los dispositivos de almacenamiento para evitar la destrucción, deterioro o alteración de los datos.

Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-m nmera@uees.edu.ec
Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-m enavides@uees.edu.ec

- Afianzar el plan de extracción de datos con un plan que contemple la priorización de las fuentes de datos y el orden en que los datos serán adquiridos

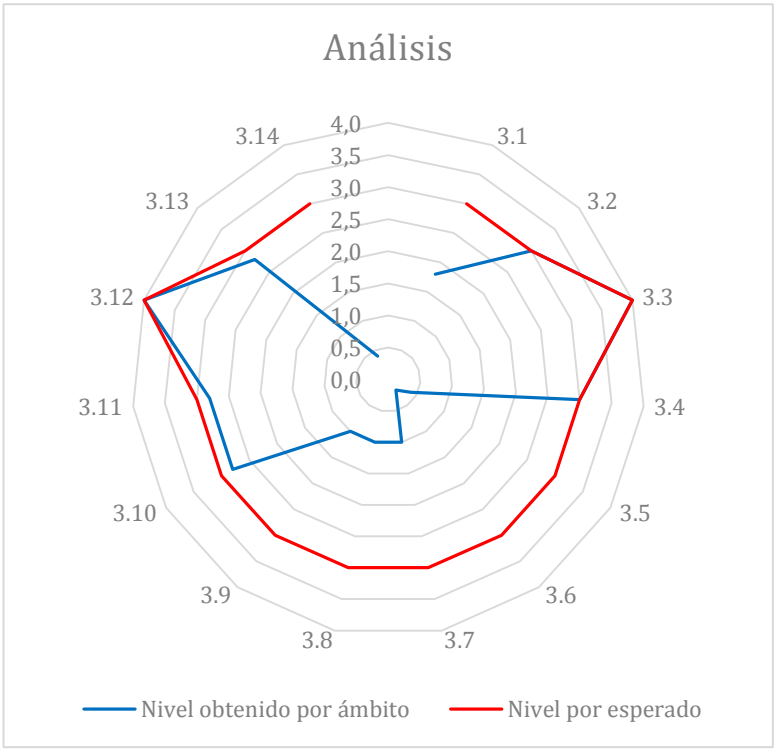
Si se detecta que el dispositivo está accediendo a datos remotos, archivos encriptados o con claves de acceso, correspondencia o comunicaciones electrónicas, datos de carácter personal entre otros se debe consultar al responsable del procedimiento acerca de los límites que pudieran existir para la captura de la información.

- Robustecer en el informe pericial con la documentación de detalles de la adquisición de datos.
- Incluir protocolos de actuación en ésta fase que incluya: **1.** determinar los posibles tipos de pruebas que se persiguen. **2.** crear un acta de levantamiento de la evidencia digital y localizar todos los equipos inalámbricos determinando todos los modos de comunicación que usan éstos. **3.**

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

ANÁLISIS

Componentes evaluados	• Establecer el orden de prioridad de la prueba que se va a examinar • Mantener notas contemporáneas detalladas y precisas de cada actuación ejecutada y los procesos que estas demandaron. • Comprobar que las evidencias no están deterioradas y son susceptibles de su estudio forense • Identificar los tipos de archivos desconocidos para determinar su valor en la investigación • Revisar los encabezados de los archivos • Especificar la hora de la BIOS del equipo informático en donde van instalados los discos duros que contienen la información de interés • Revisar los registros del sistema y de las aplicaciones que puedan estar presentes como registros de error, registros de instalación, conexión de registros, registros de seguridad entre otros. • Revisar los sellos de fechas y hora que figura en el sistema de archivos de metadatos para vincular archivos de interés. • Examinar la estructura de partición del disco para determinar si todo el tamaño físico de la unidad de disco duro se contabiliza. • Revisar nombres de archivos relevantes y patrones • Examinar las relaciones entre archivos • Estudiar la documentación adjunta a las evidencias • Considerar nuevas evidencias relevantes en el proceso que no habían sido contempladas en un principio, iniciando nuevamente la reseña de éstas, generando un nuevo proceso de gestión, custodia y trazabilidad. • Informar a quien solicitó el peritaje si se encuentra nuevas evidencias del incidente y esperar por nuevas instrucciones		
ción observad	Hallazgos Relevantes	Nivel de madurez Actual	Nivel de madurez Esperado



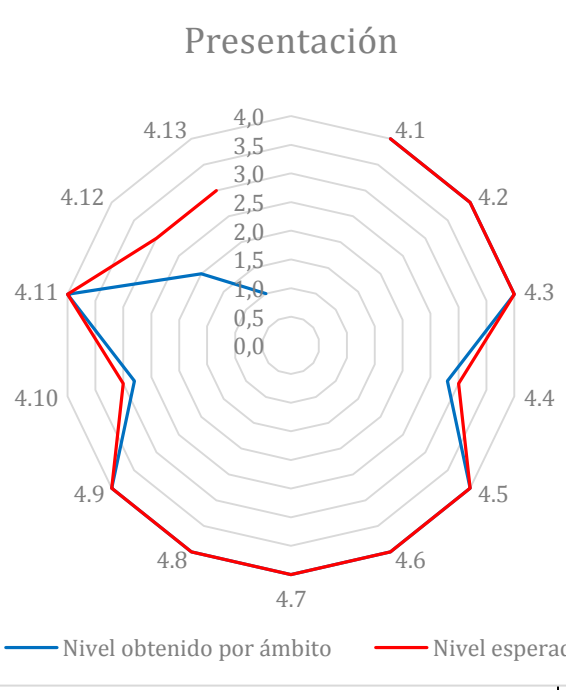
[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

	Establecer el orden de prioridad de la prueba que se va a examinar • La pericia la plasma verificando la relevancia de la información que está siendo analizada y realizando el análisis en el orden que garantice la óptima detección y recuperación de la evidencia. **Mantener notas contemporáneas detalladas y precisas de cada actuación ejecutada y los procesos que estas demandaron.** • Se registra el análisis y hallazgos del caso en el informe pericial conforme el formato proporcionado por el consejo de la judicatura y el capítulo 4 del reglamento del sistema pericial integral de la función judicial. **Comprobar que las evidencias no están deterioradas y son susceptibles de su estudio forense** • Los expertos realizan dicha comprobación **Identificar los tipos de archivos desconocidos para determinar su valor en la investigación** • La pericia se realiza identificando el tipo de evidencia a analizar **Revisar los encabezados de los archivos** • El proceso no es considerado **Especificar la hora de la BIOS del equipo informático en donde van instalados los discos duros que contienen la información de interés** • El proceso es ejecutado pero no practicado por todos los peritos **Revisar los registros del sistema y de las aplicaciones que puedan estar presentes como registros de error, registros de instalación, conexión de registros, registros de seguridad entre otros.** **Revisar los sellos de fechas y hora que figura en el sistema de archivos de metadatos para vincular archivos de interés.** **Examinar la estructura de partición del disco para determinar si todo el tamaño físico de la unidad de disco duro se contabiliza.** • Las 3 actividades anteriores no son prácticas consideradas por todos los peritos, se ejecutan de manera independiente considerado la experticia de cada perito. **Revisar nombres de archivos relevantes y**	2	3	Oportunidades de mejora	• Normalizar, socializar con los peritos y generar la documentación de los procesos relacionados con: **1.** Establecer el orden de prioridad de la prueba que se va a examinar. **2.** Identificar los tipos de archivos desconocidos para determinar su valor en la investigación. **3.** Revisar los encabezados de los archivos **4.** Revisar los registros del sistema y de las aplicaciones que puedan estar presentes como registros de error, registros de instalación, conexión de registros, registros de seguridad entre otros**. 5.** Revisar los sellos de fechas y hora que figura en el sistema de archivos de metadatos para vincular archivos de interés. **6.** Examinar la estructura de partición del disco para determinar si todo el tamaño físico de la unidad de disco duro se contabiliza. **7.** Considerar nuevas evidencias relevantes en el proceso que no habían sido contempladas en un principio, iniciando nuevamente la reseña de éstas, generando un nuevo proceso de gestión, custodia y trazabilidad. **8.** Informar a quien solicitó el peritaje si se encuentra nuevas evidencias del incidente y esperar por nuevas instrucciones • Socializar y documentar las actividades referentes a: **1.** Especificar la hora de la BIOS del equipo informático en donde van instalados los discos duros que contienen la información de interés. **2.** Revisar nombres de archivos relevantes y patrones

strante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E era@uees.edu.ec
strante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. Es avides@uees.edu.ec

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

PRESENTACIÓN			
Componentes evaluados	• Ubicar la identidad de la agencia/departamento/unidad y perito(s) que ejecutaron el análisis forense. • Ubicar el número identificador del caso, la fecha de recepción del caso y la fecha del informe • Incluir la naturaleza de los hechos investigados, la ubicación donde ocurrió la incidencia, el objetivo de la investigación, los miembros del equipo de investigación junto a sus funciones, la duración de la investigación, la ubicación de la investigación, los detalles de las pruebas digitales que se han observado durante la investigación. • Incluir una declaración clara del escritor que participó en la investigación. • Usar una plantilla de informe con formato estandarizado para ayudar a garantizar que existe suficiente información incluida en los mismos. • Detallar la información general de los dispositivos analizados, tales como marca, modelo, número de serie entre otros. • Describir brevemente las medidas adoptadas durante el examen, tales como búsquedas de cadenas, búsquedas de imágenes, gráficos y recuperar archivos borrados • Describir los programas utilizados en el análisis de la evidencia • Detallar las técnicas utilizadas • Informar si las pruebas digitales han tenido cualquier daño • Determinar los resultados y conclusiones del caso. • Incluir las limitaciones de cualquier análisis realizado • Incluir las recomendaciones para continuar con la investigación o trabajos futuros.		
ón observ	Hallazgos Relevantes	Nivel de madurez Actual	Nivel de madurez Esperado



[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

	Ubicar la identidad de la agencia/departamento/unidad y perito(s) que ejecutaron el análisis forense. **Ubicar el número identificador del caso, la fecha de recepción del caso y la fecha del informe.** **Incluir la naturaleza de los hechos investigados, la ubicación donde ocurrió la incidencia, el objetivo de la investigación, los miembros del equipo de investigación junto a sus funciones, la duración de la investigación, la ubicación de la investigación, los detalles de las pruebas digitales que se han observado durante la investigación.** • Los 3 procesos anteriores son considerados y maduros. **Incluir una declaración clara del escritor que participó en la investigación.** • En la presentación de la información general del análisis realizado no se considera ésta práctica **Usar una plantilla de informe con formato estandarizado para ayudar a garantizar que existe suficiente información incluida en los mismos.** **Detallar la información general de los dispositivos analizados, tales como marca, modelo, número de serie entre otros.** **Describir brevemente las medidas adoptadas durante el examen, tales como búsquedas de cadenas, búsquedas de imágenes, gráficos y recuperar archivos borrados.** **Describir los programas utilizados en el análisis de la evidencia** • Los 4 procesos anteriores son considerados y maduros **Detallar las técnicas utilizadas** • El proceso es considerado conforme el formato proporcionado por el consejo de la judicatura y el capítulo 4 del reglamento del sistema pericial integral de la función judicial **Informar si las pruebas digitales han tenido cualquier daño** • Se encuentra considerado en el registro del análisis y hallazgos del caso en el informe pericial pero no se registra a detalle. **Determinar los resultados y conclusiones del caso.** • El proceso es considerado y maduro **Incluir las limitaciones de cualquier análisis realizado** **Incluir las recomendaciones para continuar con la investigación o trabajos futuros.** • Los 2 procesos anteriores no son procesos estándares ejecutados por todos los peritos	3	4	Oportunidades de mejora	• Incluir una declaración clara del escritor que participó en la investigación. • Informar si las pruebas digitales han tenido cualquier daño • Incluir las limitaciones de cualquier análisis realizado • Incluir las recomendaciones para continuar con la investigación o trabajos futuros

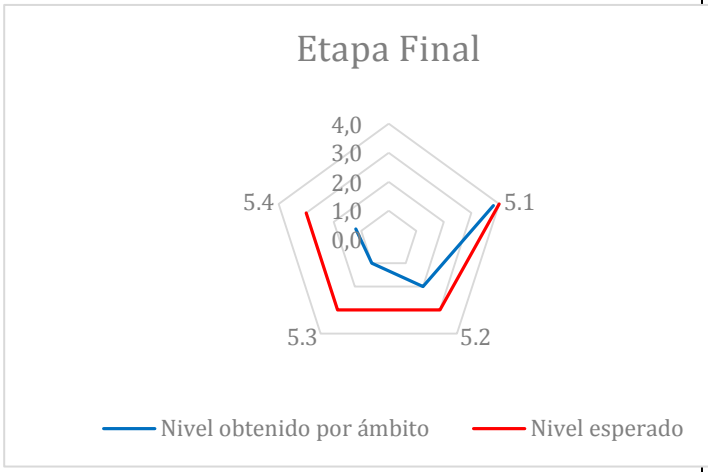
1 Estudiante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmer...ees.edu.ec
2 Estudiante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenav...@uees.edu.ec

ETAPA FINAL

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

<table>
<tr><td>Componentes evaluados</td><td colspan="3">

- Mantener una copia de la orden judicial emitida por el fiscal o juez con el expediente del caso.
- Mantener una copia de la cadena de custodia
- Documentar las irregularidades y las medidas tomadas durante el exámen
- Almacenar a largo plazo la información confidencial capturada por herramientas forenses, asegurándose que esto no infringe la privacidad de los involucrados.

</td><td colspan="2" rowspan="2"> 
</td></tr>
<tr><td rowspan="2">Situación observada</td><td>Hallazgos Relevantes</td><td>Nivel de madurez Actual</td><td>Nivel de madurez Esperado</td></tr>
<tr><td>

Mantener una copia de la orden judicial emitida por el fiscal o juez con el expediente del caso.

- Los expertos manifiestan que mantienen una copia de la orden fiscal o judicial con el expediente del caso

Mantener una copia de la cadena de custodia

- La cadena de custodia no es supervisada desde el estado previo hasta la llegada de las evidencias al entorno de análisis forense, la hoja de registro es enviada para ser firmada solo a las personas que manipulan la evidencia.

Documentar las irregularidades y las medidas tomadas durante el exámen

- Poseen solo lo documentado en el informe pericial

Almacenar a largo plazo la información confidencial capturada por herramientas forenses, asegurándose que esto no infringe la privacidad de los involucrados.

- Se guarda lo capturado para evidencias en el informe pericial

</td><td>2</td><td>3</td><td>Oportunidades de mejora</td><td>

- Mantener una copia de la cadena de custodia total
- Documentar las irregularidades y las medidas tomadas durante el exámen
- Almacenar a largo plazo la información confidencial capturada por herramientas forenses, asegurándose que esto no infringe la privacidad de los involucrados.

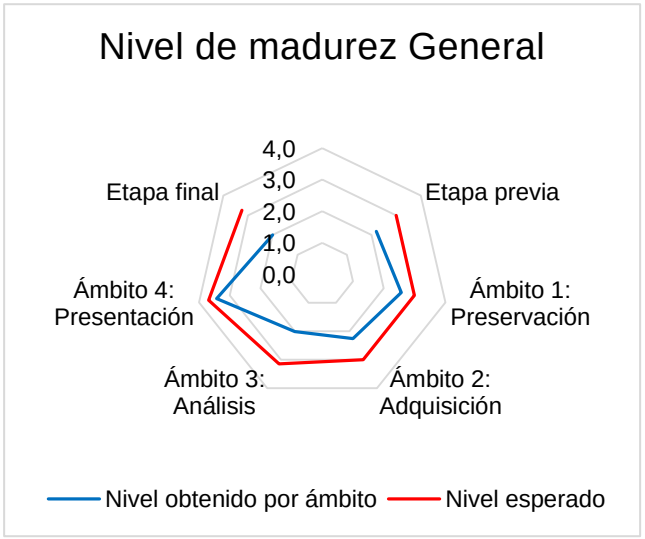
</td></tr>
</table>

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec

[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

GENERAL

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec

Componentes evaluados		Nivel de madurez Actual	Nivel de madurez Esperado	
	• Etapa Previa • Preservación • Adquisición • Análisis • Presentación • Etapa final	2,4	3	

[1] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail dmmera@uees.edu.ec
[2] Maestrante de Auditoría de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail vbenavides@uees.edu.ec