



INSTITUTO DE ALTOS ESTUDIOS NACIONALES
LA UNIVERSIDAD DE POSGRADO DEL ESTADO

REPÚBLICA DEL ECUADOR

INSTITUTO DE ALTOS ESTUDIOS NACIONALES
LA UNIVERSIDAD DE POSGRADO DEL ESTADO

Maestría en Auditoría Gubernamental y Control

Artículo Científico

**INFORMÁTICA FORENSE Y AUDITORÍA GUBERNAMENTAL,
UNA HERRAMIENTA PARA LA DETERMINACIÓN DE INDICIOS DE
RESPONSABILIDAD PENAL RELACIONADOS CON DELITOS INFORMÁTICOS.**

Autor: Stalin Xavier Caraguay Ramírez

Tutor: Dr. Fabián Guzmán Proaño

Quito, abril de 2019



No.133- 2019.

ACTA DE GRADO

En el Distrito Metropolitano de Quito, hoy a los dos días del mes de abril del año dos mil diecinueve, STALIN XAVIER CARAGUAY RAMIREZ, portador del número de cédula: 1103999973, EGRESADO DE LA MAESTRÍA EN AUDITORIA GUBERNAMENTAL Y CONTROL (2017-2019), se presentó a la exposición y defensa oral de su Artículo Científico, con el tema: "INFORMÁTICA FORENSE Y AUDITORÍA GUBERNAMENTAL. UNA HERRAMIENTA PARA LA DETERMINACIÓN DE INDICIOS DE RESPONSABILIDAD PENAL RELACIONADOS CON DELITOS INFORMÁTICOS", dando así cumplimiento al requisito, previo a la obtención del título de MAGÍSTER EN AUDITORIA GUBERNAMENTAL Y CONTROL.

Habiendo obtenido las siguientes notas:

Promedio Académico:	9.34
Artículo Científico Escrito:	8.62
Defensa Oral Artículo Científico:	8.85

Nota Final Promedio: 9.03

En consecuencia, STALIN XAVIER CARAGUAY RAMIREZ, se ha hecho acreedor al título mencionado.

Para constancia firman:

Mg. Ana Ponce.
PRESIDENTE DEL TRIBUNAL



SECRETARÍA
GENERAL

Mgs. Miguel Ángel Játiva.
MIEMBRO

Dr. Andrés Abad.
MIEMBRO

Abg. Nimena Carvajal Chiriboga.
DIRECTORA DE SECRETARÍA GENERAL

De conformidad con la facultad
prevista en el estatuto del IAN
CERTIFICO que la presente es fiel
copia del original

Foja 111

Fecha 10 JUN 2019

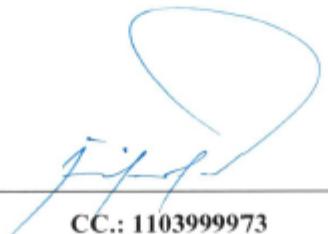
Secretaría General



INSTITUTO DE ALTOS ESTUDIOS NACIONALES
LA UNIVERSIDAD DE POSGRADO DEL ESTADO

AUTORÍA

Yo, Stalin Xavier Caraguay Ramírez, con CC 1103999973, declaro que las ideas, juicios, valoraciones, interpretaciones, consultas bibliográficas, definiciones y conceptualizaciones expuestas en el presente trabajo, así como los procedimientos y herramientas utilizadas en la investigación, son de absoluta responsabilidad del autor del trabajo de titulación. Asimismo, me acojo a los reglamentos internos de la universidad correspondientes a los temas de honestidad académica.



CC.: 1103999973



INSTITUTO DE ALTOS ESTUDIOS NACIONALES
LA UNIVERSIDAD DE POSGRADO DEL ESTADO

AUTORIZACIÓN DE PUBLICACIÓN

"Yo Stalin Xavier Caraguay Ramírez cedo al IAEN, los derechos de publicación de la presente obra por un plazo máximo de cinco años, sin que deba haber un reconocimiento económico por este concepto. Declaro además que el texto del presente trabajo de titulación no podrá ser cedido a ninguna empresa editorial para su publicación u otros fines, sin contar previamente con la autorización escrita de la universidad"

Quito, septiembre de 2018

STALIN XAVIER CARAGUAY RAMÍREZ

CC.: 1103999973

Índice

Resumen.....	1
Abstract.....	2
Introducción	4
Marco teórico.....	10
Revisión de la literatura.....	10
Evolución histórica de conceptos en contraste con la normativa ecuatoriana vigente.....	13
Estándares internacionales para la práctica de informática forense.....	15
Metodología.....	17
Análisis y discusión	20
Conclusiones.....	29
Referencias.....	32

Informática Forense y Auditoría Gubernamental,
Una Herramienta para la Determinación de Indicios de Responsabilidad Penal
Relacionados con Delitos Informáticos

Stalin Xavier Caraguay Ramírez
Instituto de Altos Estudios Nacionales

Resumen

Palabras Clave: control, información, recursos públicos, tecnología, informática forense

La Contraloría General del Estado (CGE) controla los recursos públicos mediante auditorías que ejecuta con técnicas y normas nacionales e internacionales constantes en el Manual General de Auditoría Gubernamental (MGAG) y en las Normas Ecuatorianas de Auditoría Gubernamental (NEAG), de esta manera, dado el auge de las tecnologías de la información y comunicaciones (TIC's) es importante que la CGE efectúe procedimientos de informática forense, para generar evidencia digital que sustente el cometimiento y posterior sanción de hechos ilegales en contra de los recursos estatales. Sin embargo, el problema es que ni el MGAG ni las NEAG contienen normativa expresa o procedimientos de informática forense, aun cuando son las herramientas que regulan el desarrollo de la auditoría gubernamental.

El objetivo general de este trabajo es estudiar la aplicación de la informática forense en auditorías gubernamentales como herramienta para la determinación de indicios de responsabilidad penal relacionados con delitos informáticos, en comparación con las prácticas de México y Perú, identificando las técnicas aplicables de análisis forense en materia de TIC's, analizando los delitos informáticos tipificados en el Código Orgánico Integral Penal (COIP) sobre la base del MGAG, para finalmente explicar cómo la informática forense contribuiría en los procesos de auditoría efectuados por la CGE.

La metodología empleada fue cualitativa, utilizando la técnica documental con fuentes de tipo secundarias para la recolección de información, misma que se obtuvo tanto en las organizaciones objeto de estudio como en los recursos impresos y digitales relacionados con la materia en estudio, en el marco de la línea de investigación intitulada Administración y Gestión Pública, del Centro de Gobierno y Administración Pública del Instituto de Altos Estudios Nacionales (IAEN), así como en concordancia con el eje 3 Mas Sociedad, Mejor Estado del Plan Nacional de Desarrollo 2017 – 2021. Las tres unidades de análisis fueron las experiencias que, respecto de la informática forense y la auditoría gubernamental, han desarrollado México, Perú y Ecuador, en razón de la disponibilidad de su información, y que en sus calidades de integrantes de la Organización Internacional de Entidades Fiscalizadoras Superiores (OLACEFS) aportan con el desarrollo de la comunidad en materia del control de los recursos públicos.

Resultado de la investigación se destaca que una de las técnicas de informática forense es la investigación de los sistemas informáticos, aplicando estándares internacionales tales como ISO27037, RFC3227, UNE71505 y UNE71506. Así también, se determinó que el MGAG está desactualizado ya que no guarda relación con la literatura expuesta, ocasionando que no se garantice en su totalidad el control de los recursos públicos gestionados mediante las TIC's, a diferencia de México y Perú que expidieron normativa que regula la práctica de la auditoría forense. Se revela entonces, que la contribución de la informática forense sería complementar el análisis de la evidencia digital en los procesos de auditoría efectuados por la CGE, para fortalecer el control de los recursos públicos.

Abstract

Keywords: control, information, public resources, technology, computer forensics

Public resources are controlled in the CGE, through audits with detailed national and international techniques and norms in the MGAG and NEAG, in this way, due to the boom in the TIC's, it is important that CGE implements forensic computer procedures to generate digital evidence that supports the commitment and subsequent sanction of illegal acts against state resources. However, the problem is that neither in the MGAG nor in the NEAG contain express regulations or computer forensic procedures, even though they are the tools that regulate the development of the governmental audit.

The general objective of this work is to study the application of forensic computing in government audits as a tool for the determination of evidence of criminal responsibility related to computer crimes, in comparison with the practices of Mexico and Peru, identifying the TIC's forensic analysis techniques, analyzing cybercrimes typified in the COIP on the basis of the MGAG, to finally explain how computer forensics would contribute to the auditing processes in the CGE.

The methodology used was qualitative, using the documentary technique with secondary sources for the collection of information, which was obtained in the organizations under study as in the printed and digital resources related to the subject under study, within the framework of the investigation line entitled Administration and Public Management, of the Center of Government and Public Administration of the IAEN, in accordance with axis 3 More Society, Better State of the National Development Plan 2017 – 2021. The three units of analysis were the experiences that, with respect to forensic computing and government auditing, Mexico, Peru and Ecuador have developed, because of the availability of their information, and that as members of the OLACEFS contribute with the development of the community in the control of public resources.

Result of the research shows that one of the techniques of computer forensics is the investigation of computer systems, applying international standards such as ISO27037, RFC3227, UNE71505 and UNE71506. Likewise, it was determined that the MGAG is not updated since it is not related to the exposed literature, causing that the control of public resources managed through TIC's is not completely guaranteed, unlike Mexico and Peru, which issued regulations that regulate the practice of forensic auditing. It is then revealed that the contribution of computer forensics would be to complement the analysis of digital evidence in the CGE's audit processes, in order to strengthen the control of public resources.

Introducción

En la República del Ecuador, el 3 de diciembre de 1927 se creó la Contraloría General de la Nación, denominada CGE a partir de 1967, cuya misión es controlar los recursos públicos para garantizar su uso efectivo en beneficio de los ecuatorianos (CGE, 2017), para lo cual, según lo establecido en el artículo 18 de su Ley Orgánica (LOCGE), ejecuta auditorías gubernamentales y exámenes especiales, con técnicas de auditoría y normas nacionales e internacionales (LOCGE, 2002), constantes en el MGAG (MGAG, 2003) y en las NEAG (NEAG, 2002).

La globalización evidenciada en el auge de las TIC's en la administración pública (Pardo, 2011), y el desarrollo nacional de infraestructura de telecomunicaciones, han ocasionado que progresivamente las instituciones gubernamentales de Ecuador implementen sistemas informáticos para la gestión de los recursos públicos (MINTEL, 2016), haciendo importante que la CGE, para el cumplimiento de su misión, cuente con herramientas de vanguardia como la informática forense, la cual sirve para garantizar la seguridad de la información, tiene como finalidad la prevención y corrección de infracciones, y consiste en la investigación de los sistemas informáticos para recolectar evidencia válida de su vulneración (Canedo, 2010), sin

embargo, el problema es que ni el MGAG ni las NEAG contienen normativa expresa o procedimientos de informática forense, aun cuando son las herramientas que regulan el desarrollo de la auditoría gubernamental en Ecuador.

El objetivo general de este artículo es estudiar la aplicación de la informática forense en auditorías gubernamentales como herramienta para la determinación de indicios de responsabilidad penal relacionados con delitos informáticos, en comparación con las prácticas de México y Perú, identificando las técnicas aplicables de análisis forense en materia de TIC's, analizando los delitos informáticos tipificados en el COIP sobre la base del MGAG, para finalmente explicar cómo la informática forense contribuiría en los procesos de auditoría efectuados por la CGE.

En este contexto, la interrogante planteada es ¿cómo la informática forense en la auditoría gubernamental efectuada por la CGE, contribuiría con la determinación de indicios de responsabilidad penal relacionados con delitos informáticos?

El motivo por el cual fue importante el desarrollo de esta investigación, es que con la creciente tendencia del uso de las TIC's (SNAP, 2015) surge la necesidad de aplicar técnicas de informática forense, que en conjunto con los procedimientos de auditoría ya establecidos en el MGAG, fortalezcan el control de los recursos públicos realizado mediante la auditoría gubernamental, fomentando así la eficacia, eficiencia y calidad, establecidos en el artículo 227 de la Constitución de la República como principios de la administración pública (Constitución, 2008).

Considerando que la administración pública debe minimizar riesgos en la información y proteger de ataques cibernéticos a la infraestructura estatal (SNAP, 2013), es importante la aplicación de la informática forense en auditorías gubernamentales efectuadas por la CGE, ya

que complementaría de forma integral el análisis de evidencia digital para la determinación de indicios de responsabilidad penal relacionados con delitos informáticos en las áreas de contratación pública o administrativa, ejercicio de la función pública, sistema financiero, financiamiento ilícito o camuflado de campañas electorales, administración de justicia, endeudamiento público y renegociación de deuda, entre otras (CEPAT, 2005).

De este modo, el presente trabajo de investigación pretende proporcionar un marco de referencia para la actualización del MGAG, toda vez que dicho documento no incluye técnicas y metodologías relacionadas con informática forense para ejercer un eficiente y efectivo control de los recursos públicos, en beneficio de los ecuatorianos.

La metodología empleada fue cualitativa, utilizando la técnica documental con fuentes de tipo secundarias para la recolección de información, obtenida en las organizaciones objeto de estudio y en los recursos impresos y digitales relacionados con el tema de estudio, tales como: páginas web oficiales, manuales técnicos, informes de auditoría, instrumentos legales, planes nacionales, artículos científicos, entre otros. La información fue analizada identificando similitudes, buscando diferencias y determinando equivalencias, con el fin de inferir conceptos y presentar de manera focalizada los resultados obtenidos. Las tres unidades de análisis fueron las experiencias que al respecto del tema planteado, han desarrollado México, Perú y Ecuador, justificando la selección individual sobre la base de su desarrollo macroeconómico, y utilizando para su comparación, el criterio de disponibilidad de la información, además que los tres países al formar parte de la OLACEFS, contribuyen entre sí con el desarrollo de capacidades profesionales.

Respecto de los organismos internacionales relacionados con el control de los recursos públicos, en 1953 se creó la INTOSAI Organización Internacional de Entidades Fiscalizadoras

Superiores (INTOSAI, 2018), y 10 años después, esto es en 1963 se creó la OLACEFS (OLACEFS, 2017), teniendo en común que son organismos autónomos, independientes y apolíticos, cuya finalidad es intercambiar ideas y experiencias acerca de la fiscalización y el control gubernamental, fortaleciendo la posición, competencia y prestigio de las Entidades Fiscalizadoras Superiores (EFS) que los conforman, siendo México, Perú y Ecuador miembros de estas organizaciones.

Comparando la estructura del aparato estatal, los tres países analizados cuentan con entidades gubernamentales paralelas, responsables del control y uso efectivo de los recursos públicos, así en México, la Auditoría Superior de la Federación (ASF) (LFSF, 2000); en Perú, la Contraloría General de la República (CGR) (CGR, 1929); y en Ecuador, la CGE, catalogada como organismo técnico en el artículo 211 de la Constitución de la República (Constitución, 2008).

Conceptualmente, en México la ASF definió a la auditoría forense como la modalidad de auditoría que “consiste en la aplicación de una metodología de fiscalización que conlleva la revisión rigurosa y pormenorizada de procesos, hechos y evidencias, con el propósito de documentar la existencia de un presunto acto irregular” (ASF, 2018); en contraste con Perú, la CGR estableció que la auditoría forense consiste en “obtener y analizar la información para evidenciar la ocurrencia de hechos contrarios a las normas legales y de corresponder la cuantificación del perjuicio económico, aplicando procedimientos y técnicas forenses que aseguren la preservación de la cadena de custodia” (CGR, 2015), comprobándose que ambos conceptos tienen como similitud la aplicación de procedimientos para revelar el cometimiento de delitos, sin embargo en Ecuador la CGE no ha definido en su normativa vigente el concepto de auditoría forense.

Desde el punto de vista jurídico, México y Perú han regulado el ejercicio de la informática forense en la auditoría gubernamental, teniendo que para tal efecto, en México a partir del 18 de abril de 2017 se creó en la ASF la Dirección General de Auditoría Forense (DGAF) (ASF, 2017), de igual manera Perú, siendo un país que pertenece a la Comunidad Andina (CA)¹, a través de la CGR emitió la Resolución 373-2015-CG de 31 de diciembre de 2015 (CGR, 2015), por el contrario, en Ecuador, aun cuando también pertenece a la CA, no cuenta con una unidad para la práctica de la informática forense en auditorías gubernamentales, tal como se evidencia en la estructura institucional de la CGE, definida en el artículo 5 de su Estatuto Orgánico de Gestión Organizacional por Procesos, en donde constan como procesos agradores de valor las Direcciones Nacionales de Auditoría de: Administración Central; Sectores Sociales; Deuda Pública y Finanzas; Telecomunicaciones, Conectividad y Sectores Productivos; Gobiernos Seccionales; Recursos Naturales; Salud y Seguridad Social; y, Transporte, Vialidad, Infraestructura Portuaria y Aeroportuaria (CGE, 2018).

Desde el punto de vista técnico, México y Perú normaron la aplicación de los procedimientos de informática forense en auditorías gubernamentales, de esta forma en México, la DGAF utiliza TIC's para el análisis de componentes y detección de irregularidades (ASF, 2017), así mismo en Perú, se realiza la extracción de información contenida en archivos y bases de datos, a través de técnicas que permitan su análisis, reconstrucción y validación (CGR, 2015), teniendo como similitud que, ambos países cuentan con normativa que respalda la ejecución de este tipo de análisis, a diferencia de Ecuador, cuyo orden jurídico de forma general señala que al equipo auditor se podrá incorporar personal multidisciplinario especializado de apoyo (NEAG, 2002), con la finalidad de brindar asistencia técnica en las diferentes modalidades de auditoría

¹ Colombia, Ecuador, Perú y Bolivia (Comunidad Andina, 2018)

gubernamental efectuadas por la CGE, que son: examen especial, auditoría financiera, de gestión, ambiental, y de obras públicas (LOCGE, 2002).

Aunque para la investigación pre-procesal y procesal penal, misma que no constituye auditoría gubernamental, la Fiscalía General del Estado de Ecuador (FGE) dirige el Servicio Nacional de Medicina Legal y Ciencias Forenses (SNMLCF), el cual es un organismo público especializado de carácter técnico científico adscrito al Ministerio del Interior (Correa, 2015) que efectúa pericias de informática forense (SNMLCF, 2017) definida por este organismo como el área de acción “encargada de analizar el contenido digital procedente de fuentes informáticas, electrónicas y telemáticas para la obtención de datos e información” (SNMLCF, 2018).

Desde un enfoque tecnológico, es pertinente señalar que los gobiernos de 20 de los 32 Estados de América Latina y el Caribe², integrantes de la Organización de los Estados Americanos (OEA), observaron en el año 2012, un aumento en la frecuencia de incidentes cibernéticos en comparación con el año 2011 (OEA, 2013), lo que evidencia el aumento del riesgo tecnológico al que se están expuestos los recursos públicos de México, Perú y Ecuador.

En este escenario, aun cuando las entidades de la administración pública de Ecuador implementan progresivamente el Esquema Gubernamental de Seguridad de la Información (EGSI), que contiene directrices para la gestión de la seguridad de la información (SNAP, 2013), existe la probabilidad de que la integridad de los recursos públicos se vulnere con la ocurrencia de un delito informático, que según (Arias, 2006) son actos ilícitos que se ejecutan a través de medios tecnológicos.

² Estados de América Latina y El Caribe, integrantes de la OEA: Antigua y Barbuda, Argentina, Bahamas, Barbados, Belize, Bolivia, Brasil, Chile, Colombia, Costa Rica, Dominica, Ecuador, El Salvador, Grenada, Guatemala, Guyana, Haití, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Saint Kitts y Nevis, San Vicente y las Granadinas, Santa Lucía, Suriname, Trinidad y Tobago, Uruguay, Venezuela (OEA, 2018).

Marco teórico

Revisión de la literatura.

Informática forense.

Rajesh y Ramesh (2016) definieron a la informática forense como la rama de las ciencias forenses que se ocupa de recopilar, analizar y preservar los datos de los dispositivos digitales con la finalidad de utilizarlos para resolver casos criminales y se puedan presentar como evidencia legalmente admisible en los tribunales de justicia. Así también, Matthews (2010) definió a la informática forense como el proceso de localizar, recopilar y organizar información relevante almacenada electrónicamente, utilizada generalmente en litigios, señalando que cuando dicha información se ha eliminado o es difícil de adquirir se usan frecuentemente herramientas forenses y que se puede garantizar calidad en la cadena de custodia de la evidencia electrónica, con la aplicación de buenas prácticas forenses, aspecto sumamente importante para un caso legal.

En similares términos, el Buró Federal de Investigaciones de los Estados Unidos de América (FBI) describió la informática forense como la ciencia de procesar datos electrónicos (López, Amaya, & León, 2002), concepto que se relaciona con el de auditoría informática, definida como la revisión técnica, que se efectúa a los componentes y sistemas de computación de una entidad (Muñoz, 2002). Así también, Arias (2006) precisó a la informática forense como el conjunto de técnicas y herramientas que pueden incluirse en una auditoría informática para procesar evidencia digital, facilitando así la solución de problemas relacionados con seguridad informática, obteniendo las organizaciones una respuesta para sobreponerse al cometimiento de delitos informáticos, que surgen por el uso indebido de las TIC's (Canedo, 2010).

Desde otra perspectiva, Mark y Chin (2008) conceptualizaron a la informática forense como la ciencia que engloba cuatro elementos clave en la gestión de evidencia digital, que son:

identificación, preservación, análisis y presentación; mientras que Wolfe (2003) en su definición señaló que es la profesión informática dedicada a encontrar la verdad.

Dicho esto, se infiere que la informática forense es parte de una auditoría forense, y constituye una ciencia que define métodos y procedimientos para procesar y analizar información almacenada en medios electrónicos mediante la utilización de software especializado, con la finalidad de generar evidencia suficiente, competente y pertinente, que sustente el cometimiento de hechos ilegales a ser sancionados por las entidades que efectúan auditoría gubernamental.

Auditoría gubernamental.

Villardefrancos y Rivera (2006) señalaron que la auditoría gubernamental “es ejercida por numerosas agencias gubernamentales, cuyas investigaciones, por lo general, quedan limitadas al nivel del departamento en cuestión” (pág. 4); mientras que Muñoz (2002) definió a la auditoría gubernamental como la revisión exhaustiva, sistemática y concreta que se realiza a todas las actividades y operaciones de una entidad gubernamental.

Por lo expuesto, se puede afirmar que la auditoría gubernamental es un proceso administrativo mediante el cual se analiza críticamente las acciones de los servidores públicos que administran los recursos públicos, con el fin de determinar la existencia de irregularidades, por ejemplo el cometimiento de un delito informático.

Indicio de responsabilidad penal y delito informático.

En relación al concepto de responsabilidad, Bárcenas (1995) señaló que es “la consecuencia jurídica de la violación de la ley, realizada por quien siendo imputable o inimputable, en forma activa, omisiva, dolosa o culposamente lleva a término actos previstos como ilícitos, lesionando o poniendo en peligro un bien jurídicamente tutelado” (pág. 22),

mientras que, el indicio de responsabilidad penal, se da al ocasionar daño u obtener ventajas ilícitas, originando así un delito, que debe contener los siguiente atributos: tipicidad, antijuridicidad, imputabilidad y dolo, pudiendo ser sujetos de indicios de responsabilidad penal los servidores públicos, las personas encargadas de un servicio público, así como las extrañas al referido servicio que incurran en delitos contra la administración pública (CGE, 2003).

En cuanto al delito informático, Cordova, Correa, Echerri y Pérez (2017) lo definieron como un ataque a un sitio web, sistema informático o computador, que compromete la confidencialidad, integridad o disponibilidad de un equipo informático o la información almacenada en el mismo. Así también, Clough (2011) definió las siguientes tres categorías del delito informático: (1) la computadora es el objetivo de la actividad criminal, (2) la computadora es una herramienta para cometer un delito, y (3) el uso de la computadora es un accesorio que permite evidenciar el cometimiento de un delito, teniendo en común el uso de la tecnología. Mientras que, Temperini (2013) conceptualizó al delito informático como aquellas conductas antijurídicas y actitudes ilícitas, para las cuales las computadoras son instrumento o fin. Son importantes también los dos conceptos mencionados por Ricio (2013): (1) conductas que afectan la confidencialidad integridad y disponibilidad de sistemas informáticos y/o de otros bienes jurídicos, y (2) acciones delictivas que se llevan a cabo mediante recursos informáticos.

Dicho esto, la posición del autor es que los delitos informáticos constituyen acciones ilegales ejecutadas dolosamente o por negligencia, a través de medios electrónicos, con el objeto de revelar, interceptar, eliminar, transferir, atacar, manipular, divulgar y/o vulnerar datos e información de sistemas computacionales, afectando su confidencialidad, seguridad, integridad y disponibilidad, lo que origina una responsabilidad penal, siempre y cuando dichas acciones se encuentren tipificadas y puedan ser imputables a los administradores de los recursos públicos.

Evolución histórica de conceptos en contraste con la normativa ecuatoriana vigente.

Informática forense.

La evolución de la informática forense inició en el año de 1984, fecha en la cual el FBI creó un programa conocido en la actualidad como Computer Analysis and Response Team (CART), cuyo significado en español corresponde a Equipo de Análisis y Respuesta Informática, con la finalidad de analizar delitos que se cometían utilizando medios informáticos, posteriormente en los años 90 consideró a las evidencias digitales como relevantes en un proceso de investigación, dando lugar a que en el año de 1993 se efectuó la primera conferencia internacional sobre evidencia digital, y que en el año de 1995 se funde el International Organization on Digital Evidence (IOCE), organismo que dos años después emitió un conjunto de principios, procedimientos y métodos aplicables mundialmente en el proceso de análisis de pruebas digitales (Guerra, 2014).

Al respecto, Ecuador cuenta con el SNMLCF cuya sede principal se localiza en la ciudad de Quito, teniendo como misión esta institución pública, apoyar técnicamente a la FGE, mas no a la CGE, en materia de ciencias forenses, respetando en todo momento los derechos humanos (SNMLCF, 2018).

Auditoría gubernamental.

La evolución de la auditoría se remonta a 1862, año en el cual mediante la Ley Británica de Sociedades Anónimas se reconoció por primera vez a la auditoría como profesión. Un hito importante en el desarrollo de la profesión ocurrió en Estados Unidos en el año de 1887, con la creación del American Association of Public Accountants, denominado en la actualidad Instituto Americano de Contadores Públicos Certificados, encargado de educar y proporcionar liderazgo a la comunidad de profesionales que lo conforman. Posteriormente, cuando tuvo lugar la

Revolución Industrial, a inicios del año 1900, los propietarios de empresas, a mas de requerir los servicios de administradores, demandaron los servicios de auditores como mecanismo de protección ante los fraudes financieros. Debido al crecimiento económico en Estados Unidos y Gran Bretaña, los auditores pasaron de ser descubridores de fraudes, a ser evaluadores de estados financieros tanto en empresas, bancos y entidades gubernamentales. En el año de 1987 la National Commission on Fraudulent Financial Reporting, integrada por instituciones privadas, publicó su informe proponiendo recomendaciones relacionadas al sistema de control interno, así como señalando la importancia del ambiente de control, códigos de conducta, la necesidad de disponer de comités de auditoría y auditoría interna activa y objetiva. En el año de 1992, el Committee of Sponsoring Organizations of the Treadway (COSO), integrado por instituciones privadas, publicó su informe que constituye un marco intergrado de control interno, utilizado para evaluar el control interno en organizaciones de Estados Unidos (Fonseca, 2007).

De esta manera, la normativa ecuatoriana vigente está alineada al concepto histórico de auditoría, en razón de que el artículo 18 de la LOCGE, establece que la auditoría gubernamental consiste en un sistema de asesoría y prevención de riesgos que conlleva la evaluación crítica de la administración de los recursos públicos (LOCGE, 2002).

Delito informático.

La evolución de los delitos informáticos inició con el desarrollo de las tecnologías de la información, constituyéndose en uno de los primeros ataques en la historia de internet, el programa CREEPER desarrollado por el ingeniero Bob Thomas en el año de 1971, que aunque fue catalogado como el primer virus informático, no causó ningún daño en los equipos infectados, sin embargo fue la base sobre el cual se realizó el desarrollo de ataques posteriores que ocasionaron millonarias pérdidas económicas (Loredo, 2013).

La Organización de Cooperación y Desarrollo Económico (OCDE) que es un organismo de cooperación internacional, en el año de 1983 inició un estudio para internacionalizar las leyes penales para la lucha del uso indebido de programas informáticos; publicándose en el año de 1986 un informe con normativa vigente, propuestas de reformas y una lista mínima de ejemplos de usos indebidos de dichos programas que podrían prohibirse y sancionarse; así también, en el año de 1992 la OCDE elaboró un conjunto de normas técnicas para la implementación de un marco de seguridad en los sistemas de información (Acurio, 2018).

En este sentido, la normativa ecuatoriana vigente está alineada a la evolución de delito informático, cada vez que con la vigencia del COIP, de conformidad con los artículos del 229 al 234 del Código ibídem, se sanciona penalmente el cometimiento de delitos contra la seguridad de los activos de los sistemas de información y comunicación (Asamblea, 2014).

Estándares internacionales para la práctica de informática forense.

Se describen a continuación, entre otros, los estándares mayormente aplicados en la industria de la informática forense, mismos que son factibles de implementar en entidades pública, así: la norma ISO27000 es un conjunto de directrices para garantizar la seguridad de la información, siendo parte de este conjunto, el estándar ISO27037 que establece procedimientos para identificar, recolectar, adquirir y preservar una prueba o evidencia digital para fines legales, obtenida de computadores, teléfonos celulares, dispositivos de redes de comunicaciones o medios de almacenamiento; otro estándar que regula el ámbito forense es el RFC3227 cuya finalidad es guiar los procesos para recopilar y guardar evidencia digital con criterios de orden, seguridad y privacidad que garanticen la integridad en la cadena de custodia; y, las normas UNE71505 y UNE71506 que proporcionan una metodología para la gestión, análisis y

presentación de evidencias digitales, permitiendo establecer si una infracción o incidente informático se originó con intención o por negligencia (Gervilla, 2014).

Según manda el artículo 212 de la Constitución de la República del Ecuador, son funciones de la CGE, entre otras, determinar responsabilidades administrativas, responsabilidades civiles culposas, e indicios de responsabilidad penal (Constitución, 2008), estableciéndose en el artículo 67 de la LOCGE que si producto de la auditoría gubernamental se evidencia el cometimiento de delitos que afecten los intereses del Estado y de sus instituciones, dichos resultados se remitirán a la FGE para el ejercicio de la acción penal correspondiente (LOCGE, 2002).

De esta manera, la relación de causalidad que se presenta gráficamente en la figura 1, muestra que, aplicar procedimientos de informática forense en auditorías gubernamentales, para procesar y analizar información digital, tendría un efecto positivo en la determinación de indicios de responsabilidad penal relacionados con delitos informáticos, en razón de que dichos procedimientos, generan evidencia suficiente, competente y pertinente, para sustentar hechos ilegales cometidos en contra de los recursos públicos, asegurando la posterior sanción de estos actos, tanto en la CGE como en la FGE. De esta manera se demuestra que, en la medida que la CGE regule el desarrollo de la auditoría gubernamental, incluyendo la aplicación de la informática forense, este ente de control determinaría indicios de responsabilidad penal relacionados con delitos informáticos, debidamente sustentados.

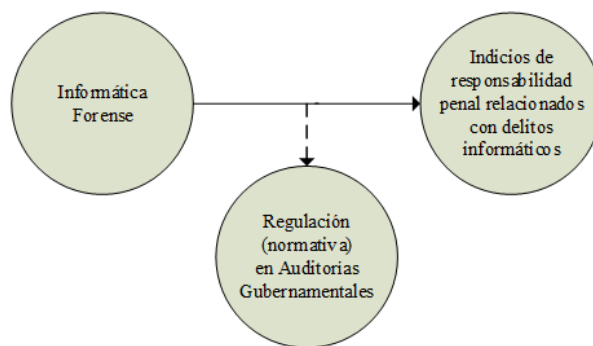


Figura 1. Relación de causalidad

Metodología

Para el desarrollo del presente artículo científico, se aplicó el método cualitativo con el objetivo de abordar a profundidad el estudio del fenómeno, investigando la aplicación de la informática forense en auditorías gubernamentales como herramienta para la determinación de indicios de responsabilidad penal relacionados con delitos informáticos; utilizando la técnica documental con fuentes de tipo secundarias para la recolección de información, misma que se obtuvo tanto en las organizaciones objeto de estudio como en los recursos impresos y digitales, tales como: páginas web oficiales de la ASF, CGR, CGE, Banco de México, FGE, INTOSAI, OLACEFS, Ministerio del Ambiente (MAE), Mexicanos Contra la Corrupción y la Impunidad (MCCI), IAEN, Banco Mundial, CA, SNMLCF, memorias oficiales de la OLACEFS y OEA, manuales técnicos de la INTOSAI, MGAG, NEAG, resoluciones de la CGR, decretos ejecutivos, informes de auditoría de la CGE, EGSI, estatutos, Plan Nacional de Gobierno Electrónico 2014-2017, Plan Nacional de Telecomunicaciones y Tecnologías de Información del Ecuador 2016-2021, Plan Nacional de Desarrollo 2017-2021, normativa como la LOCGE, COIP, Constitución del Ecuador, Ley de Fiscalización y Rendición de Cuentas de la Federación (LFRCF) y Ley de Fiscalización Superior de la Federación (LFSF) de México, Ley Orgánica del Sistema Nacional de Control (LOSNC) y Nuevo Código Procesal Penal (NCP) de Perú, libros, tesis, revistas y

artículos científicos de alto impacto; todos los recursos mencionados con información suficiente, pertinente y relevante, que sustentan los resultados del trabajo planteado.

La información fue analizada identificando similitudes, buscando diferencias, y determinando equivalencias, así como examinando a detalle y extrayendo datos relacionados con el objeto de estudio que permitieron la inferencia de conceptos y presentar de manera focalizada los resultados obtenidos, además se consideró la vigencia de las normas citadas con precisión de artículos, validando la autenticidad de los portales web, y para el caso de la conversión de pesos mexicanos (MXN) a dólares estadounidenses (USD) tomando como referencia la cotización oficial de la moneda.

Las tres unidades de análisis sobre la base de las cuales se desarrolló el trabajo de investigación fueron las experiencias que, respecto de la informática forense y la auditoría gubernamental, han desarrollado los Estados Unidos Mexicanos y las repúblicas del Perú y del Ecuador.

Se consideró los Estados Unidos Mexicanos por cuanto, siendo un país de América Latina y el Caribe, supera históricamente al producto interno bruto (PIB) de Perú y Ecuador (Banco Mundial, 2018), representándole al país norteamericano, mayores ingresos económicos que son fiscalizados por la ASF, experiencia que puede ser aprovechada por Ecuador.

De igual manera, la República del Perú es otra de las unidades de análisis en esta investigación, en razón de que, como se distingue en la figura 2, su economía expresada en el PIB, creció en los últimos 10 años con patrones similares al de nuestro país.

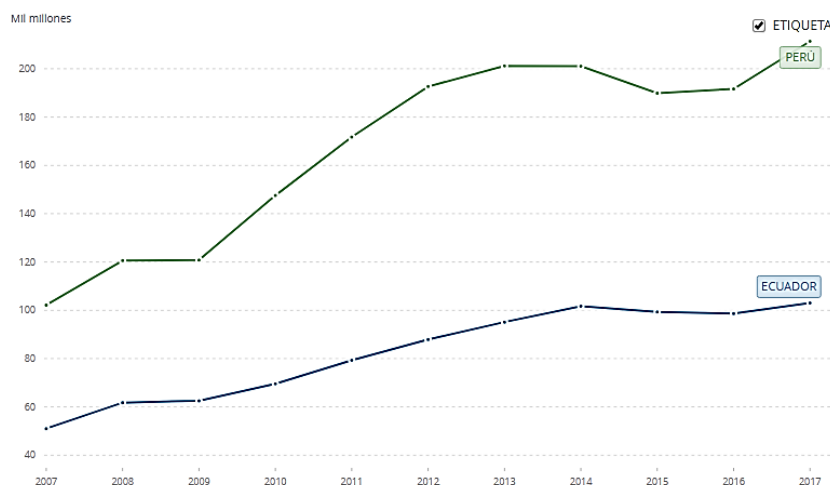


Figura 2. PIB de las repúblicas de Perú y Ecuador. Adaptado de Banco Mundial (2018).

Se comparó México, Perú y Ecuador, en razón de que son países latinoamericanos de habla hispana que, en sus calidades de integrantes de la OLACEFS, efectúan trabajos similares cuyos resultados aportan con el desarrollo de la comunidad en materia del control de los recursos públicos, de esta manera, la ASF al ser integrante del Comité de Creación de Capacidades de la OLACEFS, gestiona y promueve el desarrollo de capacidades profesionales de las demás EFS de la región, mientras que, ambas repúblicas sudamericanas integran la Comisión de las TIC's de dicho organismo internacional, que entre otros objetivos, impulsa la utilización de dichas tecnologías en las demás EFS (OLACEFS, 2017). Así también, se comparó estos tres países valorando el criterio de acceso a la información, constante en los recursos antes mencionados, en comparación con otros países de la región que no han publicado la suficiente información que permita el cumplimiento de los objetivos planteados.

Las variables objeto de comparación entre México, Perú y Ecuador, fueron la normativa vigente respecto de la informática forense en auditorías gubernamentales, así como los resultados y procedimientos que, ante el caso de delitos informáticos, adoptan cada uno de ellos.

El presente trabajo de Maestría se desarrolló en el marco de la línea de investigación intitulada Administración y Gestión Pública, del Centro de Gobierno y Administración Pública del IAEN (IAEN, 2017), en concordancia con el eje 3 Mas Sociedad, Mejor Estado del Plan Nacional de Desarrollo 2017 – 2021, que en su parte pertinente señala que en el caso de la CGE, entre otras instituciones, se debe potenciar su autonomía para investigar, determinar y sancionar la corrupción, así como fortalecer los sistemas informáticos para su detección oportuna (SENPLADES, 2017).

Análisis y discusión

Normativa sobre informática forense en auditoría gubernamental.

En la tabla 1 consta el detalle de los instrumentos legales establecidos en México, Perú y Ecuador para la práctica de la auditoría forense y consecuentemente de la informática forense en los procesos de auditoría gubernamental.

Tabla 1

Ordenamiento jurídico de auditoría forense en México, Perú y Ecuador

País	EFS	Ordenamiento Jurídico	Normativa Vigente Relacionada con Auditoría Forense
México	ASF	LFRCF	Reglamento Interior de la ASF de 16 de enero de 2017, publicado en el Diario Oficial (DO) de 20 de enero de 2017, con su reforma publicada en el DO de 13 de julio de 2018; Manual de Organización de la ASF de 18 de abril de 2017, publicado en el DO de 26 de abril de 2017
Perú	CGR	LOSNC y de la CGR; Ley de Fortalecimiento de la CGR y del Sistema Nacional de Control	Resolución 373-2015-CG de 31 de diciembre de 2015
Ecuador	CGE	LOCGE	No definida

Nota. Adaptado de la ASF, CGR y CGE

Aunque en Ecuador no existe normativa para la ejecución de auditoría forense, el MGAG emitido por la CGE contiene procedimientos que guían la ejecución de las acciones de control (MGAG, 2003) sin embargo, aun cuando se encuentra vigente, está desactualizado ya que hace referencia al derogado Código Penal, que fue reemplazado con la expedición del COIP (Asamblea, 2014), ocasionando que en el citado MGAG no hayan directrices para los casos en

los que, producto de las auditorías, se determinen indicios de responsabilidad penal relacionados con delitos informáticos, tipificados en los artículos del 229 al 234 del COIP, conforme se resumen en la tabla 2.

Tabla 2

Delitos contra la seguridad de los activos de los sistemas de información y comunicación

Artículo	Delito	Descripción	Punición
229	Revelación ilegal de base de datos	Revelar información registrada en base de datos, materializando voluntaria e intencionalmente la violación del secreto	De 1 a 3 años
		Si se comete por un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria o contratistas	De 3 a 5 años
230	Interceptación ilegal de datos	Interceptar ilegalmente un dato informático en su origen, destino o en el interior de un sistema informático	De 3 a 5 años
		Desarrollar páginas electrónicas que induzcan a ingresar a un sitio de internet diferente al que se quiere acceder	
		Clonar información de bandas magnéticas de tarjetas de pago	
231	Transferencia electrónica de activo patrimonial	Fabricación de dispositivos para clonar información	De 3 a 5 años
		Alterar el funcionamiento de sistemas informáticos para la transferencia no consentida de un activo patrimonial	
232	Ataque a la integridad de sistemas informáticos	Facilitar datos de cuenta bancaria con la intención de obtener de forma ilegítima un activo patrimonial	De 3 a 5 años
		Destruir datos informáticos	
		Diseñar dispositivos o programas informáticos para destruir datos	
233	Delitos contra la información pública reservada legalmente	Destruir o alterar infraestructura tecnológica para la transmisión de información	De 5 a 7 años
		Si se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana	De 5 a 6 años
234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	Destruir o utilizar información clasificada	De 3 a 5 años
		Utilizar cualquier medio electrónico para obtener información clasificada	De 7 a 10 años
		Cuando se comprometa gravemente la seguridad del Estado, la o el servidor público encargado de la custodia que sin la autorización revele dicha información	
		Acceder a un sistema informático para explotar ilegítimamente el acceso logrado	De 3 a 5 años

Nota. Adaptado de COIP Suplemento del Registro Oficial (RO) 180 de 10 de febrero del 2014

Procedimientos y resultados en delitos informáticos de México.

Caso la Estafa Maestra, en México.

Una investigación realizada por un grupo de periodistas independientes en México, reveló en septiembre de 2017 que, del análisis a las cuentas públicas del 2013 y 2014, se detectaron contratos ilegales por 7 mil 670 millones de MXN de los cuales se desviaron 3 mil 433 millones

de MXN, a través de la asignación de recursos federales a 8 universidades públicas, las que subcontrataron 186 empresas a las que pagaron por la adquisición de bienes y prestación de servicios, sin que dichas empresas existan, o tengan la infraestructura y personalidad jurídica para los fines que fueron contratadas (MCCI, 2018).

Acciones tomadas por la ASF.

Ante el desvío de fondos públicos derivado del caso la Estafa Maestra, la ASF inició 12 auditorías forenses en diferentes entidades públicas (MCCI, 2018), mismas que fueron ejecutadas por la DGAF, obteniendo como resultado hasta octubre de 2018, treinta denuncias penales por un perjuicio económico de 5 mil millones de MXN aproximadamente, presentadas a la Procuraduría General de la República (PGR), para la acción penal correspondiente y su posterior sanción (MCCI, 2018).

Del mismo modo, y en razón de que conforme a lo establecido en el artículo 6 de la LFRCF, la ASF fiscaliza la cuenta pública de forma posterior al término de cada ejercicio fiscal cuando el programa anual de auditoría se apruebe y publique en su página web (LFRCF, 2016), en la tabla 3 se detalla la cantidad de auditorías forenses que esta EFS realizó y aquellas que se encuentran en ejecución para la fiscalización de las cuentas públicas de los años 2009 al 2017.

Tabla 3

Auditorías forenses realizadas por la ASF

Año de la Cuenta Pública Fiscalizada	Cantidad de Auditorías Forenses
2009	7
2010	11
2011	11
2012	17
2013	14
2014	10
2015	14
2016	18
2017	11*

Nota. Adaptado de los Programas Anuales de Auditorías para la Fiscalización Superior de las Cuentas Públicas de los años del 2009 al 2017. *En proceso de ejecución.

Respecto de las auditorías forenses realizadas para la fiscalización de las cuentas públicas de los años 2009 al 2016, a continuación, en la tabla 4 se muestra la cantidad y descripción de las acciones que derivaron estos procesos, catalogándose como preventivas: la recomendación, solicitud de aclaración y pliego de observaciones, y como acciones correctivas: la promoción del ejercicio de la facultad de comprobación fiscal, promoción de responsabilidad administrativa sancionatoria y denuncia de hechos (ASF, 2018).

Tabla 4

Acciones derivadas del proceso de fiscalización

Tipo de Acción	Cantidad	Descripción
Recomendación	288	Sugerencia para mejorar los procesos administrativos y de control
Promoción del ejercicio de la facultad de comprobación fiscal	89	La ASF reporta a la autoridad competente un presunto incumplimiento fiscal
Solicitud de aclaración	56	La ASF solicita a las entidades auditadas información adicional para atender las observaciones realizadas
Promoción de responsabilidad administrativa sancionatoria	421	La ASF promueve, ante las instancias internas de control, las posibles acciones u omisiones que generarían una responsabilidad administrativa
Pliego de observaciones	577	La ASF determinará los montos de daños o perjuicios causados a la Hacienda Pública Federal o al patrimonio de los entes públicos
Denuncia de hechos	158	Denuncia penal de hechos presuntamente ilícitos con el debido sustento
Fincamiento de responsabilidad resarcitoria	180	-

Nota. Adaptado del sistema público de consultas de auditoría (ASF, 2018).

Así también, como resultado de las auditorías forenses llevadas a cabo para la fiscalización de las cuentas públicas de los años 2009 al 2016, la ASF presenta en millones de MXN los montos correspondientes a las recuperaciones que realizó, esto es el reintegro al erario federal, al patrimonio de la institución o al fondo federal correspondiente, según el caso, de los recursos empleados incorrectamente, tal como consta en la tabla 5.

Tabla 5

Recuperaciones en millones de pesos, producto de la ejecución de las auditorías forenses

Año Cuenta Pública	Determinadas	Operadas	Aclaradas	En Procedimiento Resarcitorio	Por Recuperar o Aclarar
2009	353,7	13,2	1,7	338,9	338,9
2010	337,2	29,0	82,9	225,3	225,3
2011	533,5	17,1	181,8	334,5	334,5
2012	522,1	3,1	37,4	481,6	481,6
2013	2.203,8	11,6	379,2	1501,7	1.813,0
2014	3.587,1	0,0	467,1	0	3.119,9
2015	2.937,0	0,0	41,1	0	2.895,9
2016	4.707,4	67,3	1,8	0	4.638,3
	15.181,8	141,3	1.193,1	2882,0055	13.847,4

Nota. Tomado del sistema público de consultas de auditoría (ASF, 2018).

Las recuperaciones operadas son aquellos montos que producto de los procesos de auditoría y fiscalización superior concluidos y conciliados, han sido reintegrados al erario federal (Sepúlveda, 2010). La figura 3 muestra en USD las recuperaciones operadas resultado de las auditorías forenses realizadas para la fiscalización de las cuentas públicas de los años 2009 al 2016, evidenciándose en el dominio del tiempo una tendencia ascendente de montos recuperados que alcanza la suma de USD 7 463 304,33.

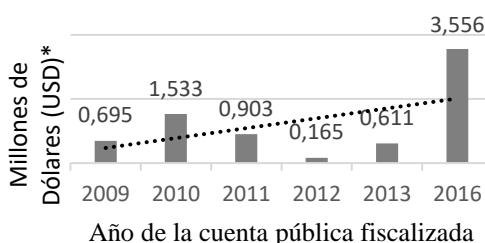


Figura 3. Montos de recuperaciones operadas expresado en millones de USD. Adaptado de ASF (2018). *Tipo de cambio oficial MXN/USD al 11/08/2018 (BANXICO, 2018).

Procedimientos y resultados en delitos informáticos de Perú.

Acciones tomadas por la CGR.

Para atender las irregularidades que afecten los recursos públicos del país andino, por ejemplo casos como la Estafa Maestra antes citado, interviene la CGR a través del Departamento de Auditoría Forense (DFOR) o quien haga sus veces, analizando los hechos para luego de ello

determinar la procedencia e inicio de una auditoría forense, con el propósito de obtener evidencia del presunto cometimiento de un delito penal, investigado paralelamente por el Ministerio Público (MP) (CGR, 2015).

En Perú, la auditoría forense concluye con la elaboración del informe pericial correspondiente y se caracteriza por ser coordinada e instrumental, en razón de que la CGR y el MP ejecutan acciones conjuntas para la obtención de evidencias que sustenten dicho informe, puesto a disposición del Fiscal responsable de la investigación una vez que finalice la acción de control (CGR, 2015).

Después de remitirse el informe pericial forense al Fiscal responsable de la investigación, fenece el principio de reserva establecido en la letra n del artículo 9 de la LOSNC, mediante el cual se prohíbe revelar información relacionada con la materia en análisis durante la ejecución de la auditoría (LOSNC, 2002), sin embargo, se mantiene la reserva y secreto de la investigación en la instancia fiscal (CGR, 2015), en cumplimiento al numeral 1 del artículo 324 del NCPP (NCP, 2004).

Por lo expuesto, aun cuando existe el sigilo de la información relacionada con los informes periciales forenses emitidos por la CGR, dado que son de carácter reservado y no han sido publicados, se presentan en esta investigación los resultados de la encuesta realizada en el año 2016 a 46 servidores públicos que desempeñan funciones administrativas financieras de una región de la República del Perú, en la cual, entre otros aspectos se les consultó si consideran necesario la implementación de una auditoría forense con el fin de contribuir en la determinación de responsabilidad penal, obteniéndose como resultado que el 80% de los encuestados respondió afirmativamente, como se demuestra en la tabla 6:

Tabla 6

Necesidad de implementar auditoría forense

Ítem	Grupos Sociales	Alternativas						Total	
		Si	%	No	%	Otros	%	Cantidad	%
1.-	Funcionarios y/o servidores públicos	37	80	7	15	2	4	46	100
	Total	37	80	7	15	2	4	46	100

Nota. Tomado de (Arohuanca, 2016).

Así también, en las tablas 7, 8, 9 y 10, respectivamente, se presentan los resultados obtenidos de otra encuesta aplicada a 44 servidores públicos, profesionales del MP, Policía Nacional del Perú y CGR, en la cual, para todos los casos, más del 86 % de los encuestados aseveraron que las evidencias de auditoría pueden demostrar la responsabilidad penal de los imputados, así como, que el cruce de información realizado por el auditor forense es trascendental en una investigación, que los movimientos financieros anómalos de una entidad son detectados en la auditoría forense y que la CGR debe incluir en su ley orgánica la implementación de auditoría forense en los organismos gubernamentales del país, tal como se muestra a continuación:

Tabla 7

Evidencias de auditoría pueden demostrar la responsabilidad penal de los imputados

Aseveración	Frecuencia	Porcentaje
Si	39	88.6
No	2	4.5
Desconoce	3	6.8
Total	44	100.0

Nota. Tomado de (Pineda, 2015).

Tabla 8

Cruce de información realizado por el auditor forense es trascendental en una investigación

Aseveración	Frecuencia	Porcentaje
Si	39	88.6
No	2	4.5
Desconoce	3	6.8
Total	44	100.0

Nota. Tomado de (Pineda, 2015).

Tabla 9

Movimientos financieros anómalos son detectados en auditoría forense

Aseveración	Frecuencia	Porcentaje
Si	38	86.4
No	2	4.5
Desconoce	4	9.1
Total	44	100.0

Nota. Tomado de (Pineda, 2015).

Tabla 10

CGR debe incluir en su ley orgánica la implementación de auditoría forense

Aseveración	Frecuencia	Porcentaje
Si	40	90.9
No	2	4.5
Desconoce	2	4.5
Total	44	100.0

Nota. Tomado de (Pineda, 2015).

Procedimientos y resultados en delitos informáticos de Ecuador.

Caso MAE.

El 24 de mayo de 2012 se detectó en el MAE el desvío de fondos públicos por 7 600 798,00 USD transferidos electrónicamente a terceros particulares mediante el uso del Sistema Integrado de Gestión Financiera (eSIGEF), hechos que fueron denunciados ante la FGE para su investigación en el ámbito penal (MAE, 2018).

Caso Gobierno Autónomo Descentralizado Municipal (GADM) del Cantón Riobamba.

Utilizando el Sistema de Pagos Interbancarios (SPI) del Banco Central del Ecuador (BCE), en abril de 2013, se desviaron electrónicamente 13 308 261,00 USD de la cuenta bancaria del GADM Riobamba a cuentas bancarias de personas particulares, sin que exista justificación alguna por la transferencia de dichos recursos públicos (CGE, 2013).

Acciones tomadas por la CGE.

Antes estos hechos similares a los ocurridos en México, respecto del desvío de recursos públicos, para el caso del MAE, el 30 de mayo de 2012 la CGE inició un examen especial mediante el cual se analizaron las transferencias que se efectuaron a cuentas bancarias de beneficiarios que no tenían relación laboral ni contractual alguna con el citado Ministerio, indicándose en los resultados de la auditoría que no fue posible identificar la dirección IP desde donde se realizaron las transferencias, ni las personas que realizaron las transacciones, así como, tampoco se identificaron los usuarios que manipularon las opciones del eSIGEF para crear en dicho sistema las cuentas beneficiarias (CGE, 2013).

Del mismo modo, para el caso del GADM del Cantón Riobamba, la CGE el 19 de abril de 2013 inició un examen especial para el análisis de operaciones, administración de identidades de cuentas de usuarios y monitoreo de transacciones electrónicas efectuadas mediante el SPI, sin embargo se excluyó de la acción de control, la revisión de los computadores y del equipamiento utilizado para acceso a internet, correo electrónico y seguridad de la información, evidenciándose que como resultado de la auditoría, tampoco se indicó las direcciones IP del origen de las transacciones, ni se pudo rastrear las operaciones electrónicas realizadas (CGE, 2013).

No obstante, para determinar si existió o no el cometimiento de un delito informático, ambos casos expuestos, también fueron motivo de análisis en la FGE, entidad que sancionó penalmente a las personas responsables. En este contexto, es apropiado citar al ex Fiscal General del Estado, actuante en los años del 2011 al 2017 (FGE, 2018), quien expresó que:

Es fundamental establecer esos nexos de cooperación, la investigación que la Contraloría realiza, el control gubernamental y que los procesos y resultados de las auditorías, al final del día, van a los jueces; por lo tanto, llevar adecuadamente una auditoría forense bien

presentada a los jueces, representará, para el trabajo de los fiscales, un apoyo inestimable en cuanto a su labor de investigar los delitos que perjudican al patrimonio del Estado.

(OLACEFS, 2012, pág. 18)

Para lo cual existen marcos de referencia relacionados con la práctica internacional de la auditoría e informática forense, por ejemplo, el manual sobre auditoría de tecnologías de la información para las EFS, que contiene buenas prácticas reconocidas universalmente y normativa aplicable en esta materia (INTOSAI, 2014).

Conclusiones

Sobre la base de la literatura expuesta, se identificaron las técnicas de informática forense aplicables en auditorías gubernamentales, para la determinación de indicios de responsabilidad penal relacionados con delitos informáticos, siendo entre otras, la investigación de los sistemas informáticos con el fin de recabar, analizar, extraer, preservar y presentar evidencia digital de su vulneración o uso en casos criminales, garantizando en todo momento, que en el marco del cumplimiento al debido proceso, no se alteren los datos de origen, con la finalidad de conservar intacta la validez de dicha evidencia posteriormente admisible en los tribunales de justicia. La investigación de los sistemas informáticos incluye también la revisión técnica, especializada y exhaustiva que se efectúa a sus instalaciones, telecomunicaciones, mobiliario y dispositivos periféricos, tanto en entornos individuales, compartidos o de redes, aplicando estándares internacionales tales como el ISO27037, RFC3227, UNE71505 y UNE71506.

De esta manera, se concluye que otra de las técnicas de informática forense identificadas, es la de localizar, recopilar y organizar información relevante almacenada electrónicamente, inclusive, con el uso de programas informáticos especializados, si ésta fue eliminada, para

garantizar calidad en la cadena de custodia de la evidencia electrónica utilizada por los administradores de justicia para sancionar el cometimiento de hechos ilegales.

Se analizaron los delitos contra la seguridad de los activos de los sistemas de información y comunicación tipificados en el COIP, sobre la base del MGAG, determinándose que dicho manual y las NEAG, aun cuando son los instrumentos legales que regulan el desarrollo de la auditoría gubernamental en el sector público ecuatoriano y dado que no contienen normativa expresa relacionada con informática forense, están desactualizados, por lo que se concluye que los mismos no guardan relación con la literatura expuesta, ocasionando que mediante los procesos normados de auditoría gubernamental no se garantice en su totalidad el control de los recursos públicos gestionados mediante las tecnologías de la información, sin embargo, debido a que, la creciente tendencia del uso de las TIC's (SNAP, 2015) incrementa el riesgo de exposición a delitos informáticos, los cuales buscan de forma ilegal afectar la confidencialidad, seguridad, integridad y disponibilidad de los sistemas computacionales y sus componentes, es necesario aplicar técnicas de informática forense que en conjunto con los procedimientos de auditoría ya establecidos en el MGAG de la CGE, fortalezcan el control de los recursos públicos, realizado mediante la auditoría gubernamental y el examen especial.

En contraste con las prácticas de México y Perú, estos países expidieron normativa que regula la práctica de la auditoría forense, contando así con una herramienta para la determinación de indicios de responsabilidad penal relacionados con delitos informáticos.

La contribución de la informática forense en la determinación de indicios de responsabilidad penal relacionados con delitos informáticos, sería complementar de forma integral el análisis de la evidencia digital en los procesos de auditoría gubernamental efectuados por la CGE, a través de la utilización de software especializado, para el control y seguimiento de

los recursos públicos en las áreas de contratación pública o administrativa, ejercicio de la función pública, sistema financiero, financiamiento ilícito o camuflado de campañas electorales, administración de justicia, endeudamiento público y renegociación de deuda (CEPAT, 2005), en concordancia con lo establecido en el EGSÍ respecto de la administración pública, que “debe propender a minimizar o anular riesgos en la información así como proteger la infraestructura gubernamental, más aún si es estratégica, de los denominados ataques informáticos o cibernéticos” (SNAP, 2013), constituyéndose esta explicación en la respuesta a la interrogante planteada.

Referencias

- Acurio, S. (10 de 2 de 2018). *Organización de los Estados Americanos*. Obtenido de Organización de los Estados Americanos:
http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
- Arias, M. (2006). Panorama General de la Informática Forense y de los Delitos Informáticos en Costa Rica. *Revista de las Sedes Regionales*, 141-154.
- Arohuanca, B. (2016). *Auditoría gubernamental y su influencia en la detección y documentación de actos de corrupción en la gestión administrativa de las municipalidades de la región Moquegua, 2014*. Tacna.
- Asamblea, N. (2014). *Código Orgánico Integral Penal*. Quito: Publicado en el Suplemento del RO 180 de 10 de febrero del 2014.
- ASF. (2017). *Manual de Organización de la Auditoría Superior de la Federación*. Ciudad de México: DO de 26 de abril de 2017.
- ASF. (20 de 07 de 2018). *ASF - Auditoría Superior de la Federación*. Obtenido de <https://www.asf.gob.mx/>
- Banco Mundial. (01 de 08 de 2018). *Portada del Banco Mundial*. Obtenido de <http://www.bancomundial.org/>
- BANXICO. (11 de 08 de 2018). *Banco de México*. Obtenido de <http://www.banxico.org.mx/>
- Bárceñas, E. (1995). Definición de la Responsabilidad ISSN: 0124-8286. *Revista Médico Legal*, 21-24.
- Canedo, A. (2010). La informática forense y los delitos informáticos. *Revista Pensamiento Americano*, 81-88.
- CEPAT. (2005). *Auditoría Forense, Herramienta de las EFS en la Lucha Contra la Corrupción*. Ecuador.
- CGE. (2003). *Manual General de Auditoría Gubernamental*. Quito.
- CGE. (2013). *Informe General DAPAYF-0006-2013*. Quito: Informes aprobados CGE.
- CGE. (2013). *Informe General DATI-0002-2013*. Quito: Informes aprobados CGE.
- CGE. (01 de 12 de 2017). *Contraloría General del Estado*. Obtenido de Contraloría General del Estado: <http://www.contraloria.gob.ec/LaInstitucion/Historia/HistoriaCGE>
- CGE. (2018). *Estatuto Orgánico de Gestión Organizacional por Procesos de la Contraloría General del Estado*. Quito: Acuerdo 0003-CG-2018 de 19 de enero de 2018 publicado en el RO Edición Especial 244 de 26 de enero de 2018.

- CGR. (1929). *Decreto Supremo de 26 de septiembre de 1929*. Lima: DO El Peruano de 2 de octubre de 1929. Obtenido de <http://www.contraloria.gob.pe/>
- CGR. (2015). *Resolución de Contraloría N° 373-2015-CG - Auditoría Forense*. Lima.
- Clough, J. (2011). Cybercrime. *Commonwealth Law Bulletin*, 671-680.
- Comunidad Andina. (20 de 07 de 2018). *Portal de la Comunidad Andina*. Obtenido de <http://www.comunidadandina.org/>
- Constitución. (2008). *Constitución de la República del Ecuador, reformada mediante enmiendas constitucionales publicadas en el RO 653 de 21 de diciembre de 2015*. Quito: Publicada en el RO 449 de 20 de octubre de 2008.
- Cordova, J., Correa, P., Echerri, F., & Pérez, J. (2017). Law versus Cybercrime. *Global Jurist*, 1-9.
- Correa, R. (2015). *Decreto Ejecutivo 759 de 27 de agosto de 2015*. Quito: Publicado en el RO Suplemento 585 de 11 de septiembre de 2015.
- FGE. (24 de 17 de 2018). <https://www.fiscalia.gob.ec/>.
- Fonseca, O. (2007). *Auditoría Gubernamental Moderna*. Lima: Editorial IICO.
- Gervilla, C. (2014). *Metodología para un Análisis Forense*. Cataluña: Repositorio Institucional de la Universidad Abierta de Cataluña.
- Guerra, C. (2014). *Análisis y aplicación de software para la recuperación forense de evidencia digital en dispositivos móviles ANDROID*. Quito.
- IAEN. (10 de 12 de 2017). *Instituto de Altos Estudios Nacionales*. Obtenido de <http://www.iaen.edu.ec/lineas-de-investigacion/>
- INTOSAI. (2014). *Manual de la IDI y del WGITA sobre auditoría de TI para las Entidades Fiscalizadoras Superiores*. Pekín, China.
- INTOSAI. (10 de 08 de 2018). *Organización Internacional de Entidades Fiscalizadoras Superiores*. Obtenido de www.intosai.org
- LFRCF. (2016). *Ley de Fiscalización y Rendición de Cuentas de la Federación*. Ciudad de México.
- LFSF. (2000). *Ley de Fiscalización Superior de la Federación*. México, D.F.
- LOCGE. (2002). *Ley Orgánica de la Contraloría General del Estado*. Quito: Publicada en el Suplemento del RO 595 de 12 de junio de 2002.
- López, O., Amaya, H., & León, R. (2002). Informática Forense: Generalidades, Aspectos Técnicos y Herramientas. *Primer Congreso Iberoamericano de Seguridad Informática CIBSI*, 2.

- Loredo, J. (2013). Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. *Celerinet*, 45.
- LOSNC. (2002). *Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República - Ley 27785*. Lima.
- MAE. (25 de 12 de 2018). *Ministerio del Ambiente*. Obtenido de <http://www.ambiente.gob.ec/el-ministerio-del-ambiente-mae-informa-en-torno-al-caso-del-desvio-de-fondos-3/>
- Mark, K., & Chin, B. (2008). Computer forensics: from the technological, procedural/organisational and legal perspectives. *International Journal of Liability and Scientific Enquiry*, 335-350.
- Matthews, D. (2010). eDiscovery versus Computer Forensics. *Information Security Journal: A Global Perspective*, 118-123.
- MCCI. (28 de 12 de 2018). *ASF interpone 7 denuncias contra Sedatu y Sedesol por presuntos desvíos*. Obtenido de <https://www.animalpolitico.com/2018/10/estafa-maestra-auditoria-denuncias-sedatu-sedesol/>
- MCCI. (27 de 12 de 2018). *La Estafa Maestra: Graduados en desaparecer dinero público*. Obtenido de <https://www.animalpolitico.com/estafa-maestra/>
- MGAG. (2003). *Manual General de Auditoría Gubernamental*. Quito: Acuerdo 012-CG-2003 de 6 de junio de 2003, publicado en el RO 107 de 19 de junio de 2003.
- MINTEL. (2016). *Plan Nacional de Telecomunicaciones y Tecnologías de Información del Ecuador 2016-2021*. Quito: Acuerdo ministerial 7 de 26 de abril de 2016, publicado en el RO Suplemento 783 de 24 de junio de 2016.
- Muñoz, C. (2002). *Auditoría en sistemas computacionales*. México: Pearson Educación.
- NCPP. (2004). *Nuevo Código Procesal Penal - Decreto Legislativo 957*. Lima.
- NEAG. (2002). *Normas Ecuatorianas de Auditoría Gubernamental*. Quito: Acuerdo 19 CG de 5 de septiembre de 2002, publicado en el RO Suplemento 6 de 10 de octubre de 2002.
- OEA. (2013). *Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos*. Washington, D.C.
- OEA. (enero de 2018). *Organización de los Estados Americanos*. Obtenido de <http://www.oas.org/es/>
- OLACEFS. (2012). La auditoría forense fortalece el trabajo de las EFS. *OLACEFS*, 18.
- OLACEFS. (19 de 12 de 2017). *Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores*. Obtenido de <http://www.olacefs.com>
- Pardo, L. (2011). Aplicación de las nuevas tecnologías en la administración pública. *Revista de Contabilidad y Dirección*, 105-126.

- Pineda, G. (2015). *Efectos de la auditoría forense en la investigación del delito de lavado de activos en el Perú, 2013 - 2014*. Lima.
- Rajesh, K., & Ramesh, K. (2016). Computer Forensics: An Overview. *i-Manager's Journal on Software Engineering*, 1-5.
- Rico, M. (2013). Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los. *IUS. Revista del Instituto de Ciencias Jurídicas*, 207-222.
- SENPLADES. (2017). *Plan Nacional de Desarrollo 2017-2021*. Quito.
- Sepúlveda, I. (2010). La Auditoría Superior de la Federación: un órgano para la rendición de cuentas. *Revista Electrónica del Centro de Estudios en Administración Pública de la Facultad de Ciencias Políticas y Sociales, Universidad Nacional Autónoma de México*, 1-16.
- SNAP. (2013). *Esquema Gubernamental de Seguridad de la Información*. Quito: Acuerdo Ministerial 166 de 19 de septiembre de 2013, publicado en el RO Suplemento 88 de 25 de septiembre de 2013.
- SNAP. (2015). *Plan Nacional de Gobierno Electrónico 2014-2017*. Quito.
- SNMLCF. (2017). *Servicio de Medicina Legal y Ciencias Forenses, Estatuto Orgánico*. Quito.
- SNMLCF. (10 de 02 de 2018). *Servicio Nacional de Medicina Legal y Ciencias Forenses*. Obtenido de Servicio Nacional de Medicina Legal y Ciencias Forenses: <https://www.cienciasforenses.gob.ec/mision-vision/>
- SNMLCF. (20 de 07 de 2018). *SNMLCF - Servicio Nacional de Medicina Legal y Ciencias Forenses*. Obtenido de <https://www.cienciasforenses.gob.ec/servicios-de-criminalistica/>
- Temperini, M. (2013). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. *1er. Congreso Nacional de Ingeniería Informática/Sistemas de Información*, 1-12.
- Villardefrancos, M. d., & Rivera, Z. (2006). La auditoría como proceso de control: concepto y tipología. *Ciencias de la Información*, 4.
- Wolfe, H. (2003). Computer forensics. *Computers & Security*, 26-28.