Estado & comunes, revista de políticas y problemas públicos
ISSN: 1390-8081
ISSN: 2477-9245
Instituto de Altos Estudios Nacionales (IAEN)

Caraguay Ramírez, Stalin Xavier

Aplicación de informática forense en auditorías gubernamentales para la determinación de indicios de responsabilidad penal con delitos informáticos en Ecuador, México y Perú, 2007-20191

Estado & comunes, revista de políticas y problemas públicos, vol. 2, núm. 11, 2020, Julio-Diciembre, pp. 135-153
Instituto de Altos Estudios Nacionales (IAEN)

DOI: https://doi.org/10.37228/estado_comunes.v2.n11.2020.178

Disponible en: https://www.redalyc.org/articulo.oa?id=684272391007

Coyuntura

Aplicación de informática forense en auditorías gubernamentales para la determinación de indicios de responsabilidad penal con delitos informáticos en Ecuador, México y Perú, 2007-2019[1]

Application of Forensic Computing in Government Audits for the Determination of Trace of Criminal Responsibility with Computer Crimes in Ecuador, Mexico and Peru, 2007-2019

Stalin Xavier Caraguay Ramírez

Consultor independiente, Ecuador

Correo electrónico: sxavyer@hotmail.com

Orcid: https://orcid.org/0000-0001-6027-786X

Recibido: 28-mayo-2019. Aceptado: 6-febrero-2020.

Resumen

El objetivo de este artículo es comparar la aplicación de la informática forense en auditorías gubernamentales, herramienta para la determinación de indicios de responsabilidad penal relacionados con delitos informáticos, en Ecuador, México y Perú. Enfatizamos el caso ecuatoriano al identificar las técnicas aplicables de análisis forense en materia de tecnologías de la información y comunicación. Analizamos los delitos informáticos tipificados en el Código Orgánico Integral Penal (COIP) sobre la base del Manual General de Auditoría Gubernamental (MGAG) y en las Normas Ecuatorianas de Auditoría Gubernamental (NEAG) para luego, por último, explicar cómo la informática forense contribuye en los procesos de auditoría efectuados por la Contraloría General del Estado (CGE). Este artículo acude al método comparativo mediante el uso de documentación normativa,

1 Este artículo contiene elementos de la investigación titulada "Informática forense y auditoría gubernamental, una herramienta para la determinación de indicios de responsabilidad penal relacionados con delitos informáticos", realizada en el Instituto de Altos Estudios Nacionales (IAEN) para la obtención del grado de magíster en Auditoría Gubernamental y Control, cohorte 2017-2019.

Estado & comunes, revista de políticas y problemas públicos. N.° 11, vol. 2, julio-diciembre 2020, pp. 135-153.
Instituto de Altos Estudios Nacionales (IAEN). Quito-Ecuador.
ISSN impreso: 1390-8081 - ISSN electrónico: 2477-9245

legal y científica para identificar las similitudes, diferencias y equivalencias de los tres casos presentados.

Palabras clave: informática forense, auditorías gubernamentales, Contraloría General del Estado, indicios de responsabilidad penal, Código Orgánico Integral Penal.

Abstract

The aim of this article is to compare the application of forensic informatics in government audits, a tool for determining indications of criminal responsibility related to computer crimes, in Ecuador, Mexico and Peru. We emphasise the Ecuadorian case by identifying the applicable forensic analysis techniques in the field of information and communication technologies. We analyse computer crimes typified in the COIP on the basis of the MGAG and the NEAG to finally explain how forensic informatics contributes to the audit processes carried out by the CGE. This article uses the comparative method through the use of normative, legal and scientific documentation to identify the similarities, differences and equivalences of the three cases here presented.

Keywords: computer forensics, government audits, Office of the Comptroller General of the State, evidence of criminal responsibility, Organic Criminal Code.

1. Introducción

El 3 de diciembre de 1927 se creó la Contraloría General de la Nación (CGE) de Ecuador, cuya misión ha sido controlar los recursos públicos para garantizar su uso efectivo en beneficio de los ecuatorianos (CGE, 2017). Según lo establecido en el artículo 18 de su Ley Orgánica, la CGE ejecuta auditorías gubernamentales y exámenes especiales constantes con técnicas y normas nacionales e internacionales presentes en el Manual General de Auditoría Gubernamental (MGAG, 2003) y en las Normas Ecuatorianas de Auditoría Gubernamental (NEAG, 2002). La CGE cuenta con distintas herramientas, entre ellas, la informática forense, la cual garantiza la seguridad de la información, prevención y corrección de infracciones mediante la investigación de los sistemas informáticos para recolectar evidencia válida de su vulneración (Canedo, 2010). Sin embargo, el problema es que el MGAG y las NEAG, aun cuando son las herramientas que regulan el desarrollo de la auditoría gubernamental en Ecuador, no contienen normativa expresa o procedimientos de informática forense que hacen parte de la auditoría forense.

El auge de las tecnologías de la comunicación y la información (TIC) en la Administración pública (Pardo, 2011) y el desarrollo de la infraestructura de telecomunicaciones han hecho que las instituciones públicas de Ecuador, entre otras medidas, implementen sistemas informáticos para la gestión de sus recursos (Ministerio de Telecomunicaciones y de la Sociedad de la Información [Mintel], 2016). Sobre todo, después de que veinte de los treinta y dos Gobiernos que integran la Organización de los Estados Americanos (OEA) observaran en el año

2012 un aumento en la frecuencia de incidentes cibernéticos en comparación con el año 2011 (OEA, 2013), siendo el mínimo incremento reportado entre el 8 % y el 12 % y un incremento máximo del 40 %, lo que evidencia el riesgo tecnológico al que se encuentran expuestos los recursos públicos.

Pese a que las entidades públicas de Ecuador implementan el Esquema Gubernamental de Seguridad de la Información (EGSI), que contiene directrices para la gestión de la seguridad de la información (Secretaría Nacional de Administración Pública [SNAP], 2013), existe la probabilidad de que la integridad de los recursos públicos se vulnere con la ocurrencia de un delito informático que, según Michael Arias (2006), son actos ilícitos que se ejecutan mediante medios tecnológicos.

En países como México, regulado por la Auditoría Superior de la Federación (ASF), la modalidad de auditoría forense existe y "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). Mientras que en Perú esta modalidad procura "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" (Contraloría General de la República [CGR], 2015).

Desde la normativa jurídica, México y Perú han regulado el ejercicio de la informática forense en la auditoría gubernamental. México lo hace mediante la Dirección General de Auditoría Forense (DGAF) y Perú mediante la Directiva de Auditoria Forense. Por su parte, Ecuador 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 Contraloría, definida en el Estatuto Orgánico de Gestión Organizacional por Procesos.

En México, la DGAF utiliza a las TIC para el análisis de componentes y detección de irregularidades (ASF, 2017), mientras que en Perú la extracción de información contenida en archivos y bases de datos se realiza con técnicas como la observación, inspección, conciliación, preservación, recuperación, reconstrucción de archivos, entre otras (CGR, 2015). Esto contrasta con el ordenamiento jurídico de Ecuador, el cual señala que al equipo auditor se podrá incorporar personal multidisciplinario especializado de apoyo (CGE, 2002) con la finalidad de brindar asistencia técnica en las diferentes modalidades de auditoría gubernamental efectuadas por la CGE, que son el examen especial y las auditorías financiera, de gestión, ambiental y de obras públicas (CGE, 2002).

Hay que aclarar que, para la investigación preprocesal y procesal penal, la Fiscalía General del Estado de Ecuador (FGE) dirige el Servicio Nacional de Medicina Legal y Ciencias Forenses (SNMLCF), organismo público especializado de carácter técnico científico adscrito al Ministerio del Interior (SNMLCF, 2015),

que efectúa pericias de informática forense pero en ningún momento se constituye como herramienta de auditoría gubernamental. La Fiscalía define al SNMLCF 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).

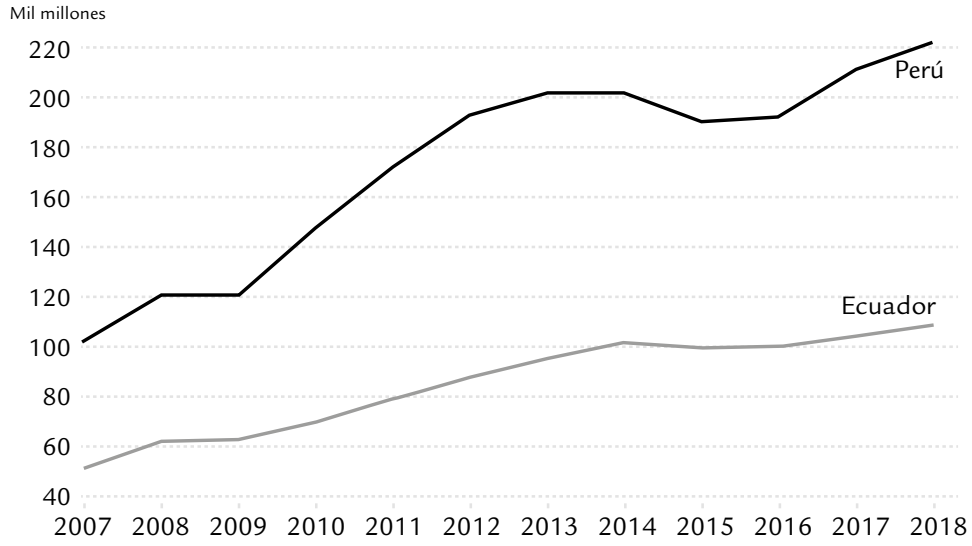
Considerando que la Administración pública debe minimizar los riesgos en la información y proteger de ataques cibernéticos a la infraestructura estatal (SNAP, 2013), resulta importante la aplicación de la informática forense, ya que complementaría el análisis de la evidencia digital para la determinación de indicios de responsabilidad penal relacionados con delitos informáticos en diferentes áreas de la Administración pública (Comisión Técnica Especial de Ética Pública, Probidad Administrativa y Transparencia [Cepat], 2005).

Por lo anterior, el objetivo de este artículo es indagar cómo la aplicación de la informática forense en auditorías gubernamentales se constituye en una herramienta para la determinación de indicios de responsabilidad penal relacionados con delitos informáticos, tomando por casos de estudio a los países de México, Perú y Ecuador, haciendo énfasis en este último. Para dar respuesta se aplicó el método comparativo mediante el análisis de información normativa y legal obtenida de las páginas web de las instituciones públicas objeto de estudio (ASF, CGE, CGR), memorias oficiales de organizaciones reguladoras y fiscalizadoras (Intosai, MCCI, Olacefs), informes de entidades internacionales (Banco Mundial, OEA), decretos ejecutivos, códigos procesales (COIP), entre otros. En dichos documentos se identificaron similitudes, diferencias y se extrajeron datos de las tres experiencias que han demostrado la incidencia de la informática forense en auditorías gubernamentales.

Se escogieron los casos de México, Perú y Ecuador, en razón de que son países de habla hispana que integran la Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores (Olacefs) y que han reportado de forma constante e ininterrumpida sus resultados en materia de control de los recursos públicos. De esta manera, la ASF en México gestiona y promueve el desarrollo de las capacidades profesionales de las demás entidades fiscalizadoras superiores (EFS) de la región, mientras que Perú y Ecuador, al integrar la comisión de las TIC de la Olacefs, impulsan la utilización de dichas tecnologías en las demás EFS (Olacefs, 2017). Además, se realizó esta comparación valorando el criterio de acceso a la información, tales como base legal y cifras de valores recuperados, en comparación con otros países de la región que no han publicado la suficiente información que permita el cumplimiento de los objetivos aquí planteados.

Además, la selección de los tres países obedece a varias razones: 1) México reporta los mayores ingresos económicos de la región (Banco Mundial, 2018), por lo que la ASF tiene un gran reto en la fiscalización; y 2) Perú y Ecuador son países que pertenecen a la Comunidad Andina, y como se distingue en el gráfico 1, ambas economías, expresadas en el PIB, crecieron en los últimos diez años con patrones similares.

Grafico 1
PIB de Perú y Ecuador, 2007-2018



Fuente: adaptado de Banco Mundial (2018).

1.1 Evolución histórica conceptual

La evolución de la auditoría se remonta al año 1862, cuando la Ley Británica de Sociedades Anónimas reconoció por primera vez a la auditoría como profesión. Un hito importante en el desarrollo de la profesión ocurrió en Estados Unidos en 1887 con la creación del American Association of Public Accountants, denominado en la actualidad American Institute of Certified Public Accountants, encargado de educar y proporcionar liderazgo a la comunidad de profesionales que lo conforman. A inicios de la primera década del siglo xx, 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, como en bancos y entidades gubernamentales.

En el año de 1987, la National Commission on Fraudulent Financial Reporting, integrada por instituciones privadas, publicó su informe en el que propuso recomendaciones relacionadas con el sistema de control interno, 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 publicó su informe, el cual constituye un marco integrado de control interno, utilizado para evaluar el control interno en organizaciones de Estados Unidos (Fonseca, 2007). De este modo, la normativa

ecuatoriana vigente se encuentra alineada al concepto histórico de auditoría, ya 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 (CGE, 2002).

En la década de 1970, en Estados Unidos los criminales empiezan a utilizar nuevos medios y conocimientos para actos vandálicos, tales como sabotaje, derechos de autor y modificación de datos, ante lo cual y para contrarrestar estas acciones surge la informática forense en el año de 1984, a cargo del Buró Federal de Investigaciones (FBI, por sus siglas en inglés), el cual creó el programa Computer Analysis and Response Team (CART) con la finalidad de analizar delitos que se cometían utilizando medios informáticos. Tiempo después, en la década de 1990, el FBI consideró a las evidencias digitales como relevantes en un proceso de investigación, dando lugar a la primera conferencia internacional sobre evidencia digital en el año 1993 y a la fundación del International Organization on Digital Evidence (IOCE) en 1995, organismo que emitió un conjunto de principios, procedimientos y métodos aplicables a escala mundial, incluido América Latina, en el proceso de análisis de pruebas digitales (Guerra, 2014).

Ecuador, para garantizar la seguridad ciudadana y el orden público dentro del territorio nacional, así como para prevenir la comisión de delitos, emitió en el 2001 el Reglamento de la Policía Judicial. Además, desde el año 2015 el país cuenta con el Servicio Nacional de Medicina Legal y Ciencias Forenses (SNMLCF), que tiene por misión el apoyo técnico a la Fiscalía General del Estado (FGE), mas no a la CGE, en materia de ciencias forenses, respetando en todo momento los derechos humanos (Servicio Nacional de Medicina Legal y Ciencias Forenses [SNMLCF], 2018).

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 la cual se realizó el desarrollo de ataques posteriores que ocasionaron millonarias pérdidas económicas (Loredo, 2013). La Organización de Cooperación y Desarrollo Económico (OCDE) en el año de 1983 inició un estudio para internacionalizar las leyes penales en la lucha del uso indebido de programas informáticos, el cual se publicó en el año de 1986. El informe contiene una normativa, 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 1992 la OCDE elaboró un conjunto de normas técnicas para implementar un marco de seguridad en los sistemas de información (Acurio, 2018). En tal sentido, la normativa ecuatoriana vigente se encuentra alineada a la evolución descrita de delito informático, toda vez que el Código Orgánico Integral Penal (COIP) vigente, de conformidad con los artículos del 229 al 234, sanciona desde lo penal el cometimiento de delitos contra la seguridad de los activos de los sistemas de información y comunicación (Asamblea Nacional, 2014).

2. Relación entre informática forense, auditoría gubernamental, indicio de responsabilidad penal y delito informático

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 que se puedan presentar como evidencia admisible en el ámbito legal en los tribunales de justicia. Así también, Matthews (2010) la definió como el proceso de localizar, recopilar y organizar información relevante almacenada de forma electrónica, utilizada por lo general en litigios. Dicho autor señala que en el momento en que esta información se ha eliminado o es difícil de adquirir, por lo que se utilizan herramientas forenses para recuperarlas, pudiendo garantizarse la calidad en la cadena de custodia de la evidencia electrónica con la aplicación de buenas prácticas forenses, aspecto importante para un caso legal.

En similares términos, el FBI describió la informática forense como la ciencia encargada de procesar datos electrónicos (López, Amaya y 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) definió 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, sobre todo para las organizaciones que necesitan de una respuesta para sobreponerse al cometimiento de delitos informáticos que surgen por el uso indebido de las TIC (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 conceptualización, señaló que es la profesión de informática dedicada a encontrar la verdad. Dicho esto, se entiende a la informática forense como 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 un *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.

Villardefrancos y Rivera (2006, p. 4) señalaron que la auditoría gubernamental "es ejercida por numerosas agencias gubernamentales, cuyas investigaciones, por lo general, quedan limitadas al nivel del departamento en cuestión", mientras que Muñoz (2002) la definió 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 con sentido crítico las acciones de los servidores públicos que administran los recursos públicos, con el fin de determinar la existencia de irregularidades, que puede ser por ejemplo el cometimiento de un

delito informático, el cual es definido por Córdova, Correa, Echerri y Pérez (2017) 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. Estos actos, de ser comprobados, dan lugar a un indicio de responsabilidad penal, ya que generan daño o se obtiene ventajas ilícitas de su uso. Para que dichos actos constituyan delito, deben tener algunas características, entre las cuales están: tipicidad,[2] antijuridicidad,[3] imputabilidad[4] y dolo[5] (CGE, 2003). Por ende, son sujetos de indicios de responsabilidad 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).

Con lo expuesto se infiere que los delitos informáticos constituyen acciones ilegales ejecutadas con dolo o por negligencia, mediante dispositivos electrónicos, con el objeto de revelar, interceptar, eliminar, transferir, atacar, manipular, divulgar o vulnerar datos e información de sistemas computacionales, afectando su confidencialidad, seguridad, integridad y disponibilidad. Esto origina una responsabilidad penal, siempre y cuando dichas acciones se encuentren tipificadas y puedan ser imputables a los administradores de los recursos públicos.

3. Estándares internacionales para la práctica de informática forense

Se describen a continuación, entre otros, los estándares aplicados en su mayoría en la industria de la informática forense, mismos que son factibles de implementar en entidades públicas. Así, la norma ISO27000, emitida por la Organización Internacional de Normalización, es un conjunto de directrices que garantizan 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, emitido por la organización internacional Grupo de Trabajo de Ingeniería de Internet, 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, emitidas por la Asociación Española de Normalización, que proporcionan una metodología para la gestión, análisis y presentación de evidencias digitales que permiten 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 (CRE), son funciones de la CGE, entre otras, determinar responsabilidades

2 Adecuación del hecho que se considera delito al tipo descrito en la ley (Márquez, 1992).

3 Conducta contraria al derecho (Zambrano, 2009).

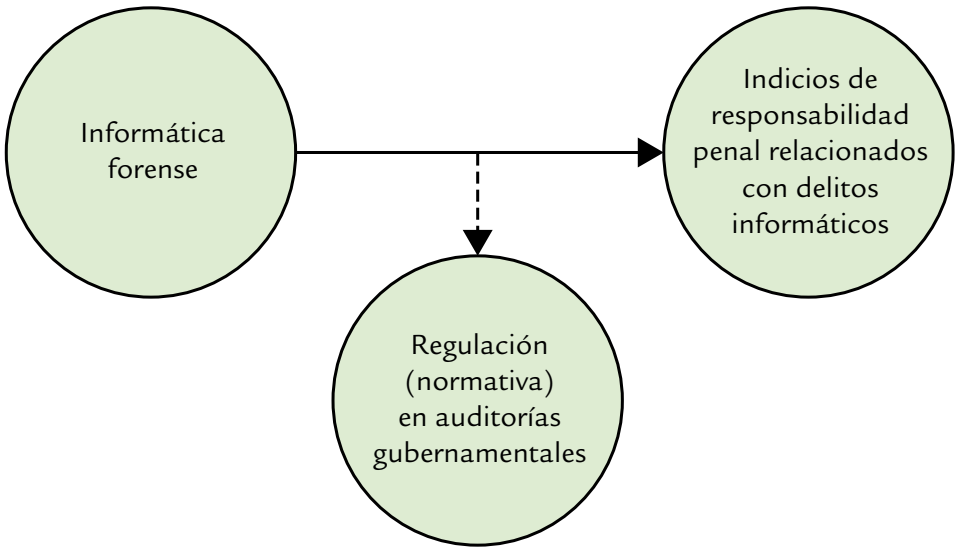
4 Atribuir a una persona las consecuencias de sus actos (González, 1995).

5 Voluntad de cometer un hecho ilícito de manera intencional (Zárate & Eleuterio, 2019).

administrativas, civiles culposas e indicios de responsabilidad penal (CRE, 2008). El artículo 67 de la LOCGE establece que, si durante 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 (CGE, 2002).

De esta manera, la relación de causalidad que se presenta en el gráfico 2 nos permite afirmar que aplicar en auditorías gubernamentales los procedimientos de informática forense observando los estándares internacionales ISO27037, RFC3227, UNE71505 y UNE71506, con la finalidad de procesar y analizar información digital, tendría un efecto positivo en la determinación de indicios de responsabilidad penal relacionados con delitos informáticos. Esto en razón de que dichos procedimientos aseguran que la evidencia sea suficiente, competente y pertinente, para sustentar hechos ilegales cometidos en contra de los recursos públicos, objeto de sanción a la que hubiere lugar tanto en la CGE como en la FGE. En la medida en que la CGE regule el desarrollo de la auditoría gubernamental, incluyendo la aplicación de la informática forense, este ente de control complementaría la determinación de indicios de responsabilidad penal relacionados con delitos informáticos, sustentados de manera debida.

Gráfico 2
Relación de causalidad



Fuente: elaboración propia del autor (2017).

4. Normativa sobre informática forense en auditoría gubernamental

En la tabla 1 se exponen los instrumentos legales establecidos en México y Perú para la práctica de la auditoría forense y, de manera consecuente, de la informática forense en los procesos de auditoría gubernamental, con el fin de evidenciar que en Ecuador no se ha definido un marco jurídico para la práctica indicada.

Tabla 1

Ordenamiento jurídico de auditoría forense en México, Perú y Ecuador

País	Normativa vigente relacionada con auditoría forense
México	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	Resolución 373-2015-CG de 31 de diciembre de 2015
Ecuador	No definida

Fuente: elaboración propia del autor (2017).

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 (CGE, 2003). Sin embargo, pese a que dicho manual se encuentra vigente, el mismo se encuentra desactualizado ya que hace referencia al derogado Código Penal que fue reemplazado con la expedición del COIP (Asamblea Nacional [AN], 2014). El MGAG no contiene 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 en Ecuador

Artículo	Delito	Punición
229	Revelación ilegal de base de datos	1 a 5 años
230	Interceptación ilegal de datos	3 a 5 años
231	Transferencia electrónica de activo patrimonial	3 a 5 años
232	Ataque a la integridad de sistemas informáticos	3 a 7 años
233	Contra la información pública reservada legalmente	5 a 10 años
234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	3 a 5 años

Nota. Adaptado de COIP, Suplemento del Registro Oficial (RO) 180 de 10 de febrero del 2014.
Fuente: elaboración propia del autor (2017).

5. Procedimientos y resultados en delitos informáticos

5.1. El caso de México

Una investigación publicada en septiembre de 2017 por un grupo de periodistas independientes en México reveló que en las cuentas públicas del 2013 y 2014 había contratos ilegales por un valor total de 7670 millones de pesos mexicanos (MXN), de los cuales se desviaron 3433 millones de MXN mediante la asignación de recursos federales a ocho universidades públicas. Estas, a su vez, subcontrataron a 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. Este caso es conocido como la Estafa Maestra (Mexicanos Contra la Corrupción y la Impunidad [MCCI], 2018).

Ante el desvío de estos fondos públicos, la ASF inició doce auditorías forenses en diferentes entidades públicas (MCCI, 2018), las mismas que fueron ejecutadas por la DGAF, que, como se explicó, utiliza a las TIC para el análisis de componentes y detección de irregularidades, obteniendo por resultado, hasta octubre de 2018, cerca de treinta denuncias penales por perjuicio económico de cerca de 5000 millones de MXN, denuncias presentadas ante la Procuraduría General de la República (PGR) para la acción penal correspondiente y su posterior sanción (MCCI, 2018).

Amparados en el artículo 6 de la Ley de Fiscalización y Rendición de Cuentas de la Federación (LFRCF), la ASF fiscaliza la cuenta pública al término de cada ejercicio fiscal en el momento en que el programa anual de auditoría se apruebe y publique en su página *web* (Cámara de Diputados, 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

Nota: adaptado de los Programas Anuales de Auditorías para la Fiscalización Superior de las Cuentas Públicas de los años del 2009 al 2017.

Fuente: elaboración propia del autor (2017).

Respecto de las auditorías forenses, la tabla 4 evidencia la cantidad y descripción de las acciones preventivas que se derivaron de estos procesos, tales como la recomendación, solicitud de aclaración y pliego de observaciones. Mientras que entre las acciones correctivas tenemos la promoción del ejercicio de la facultad de comprobación fiscal, promoción de responsabilidad administrativa sancionatoria y denuncia de hechos (Auditoría Superior de la Federación [ASF], 2018).

Tabla 4

Acciones derivadas del proceso de fiscalización

Tipo de acción	Cantidad
Recomendación	288
Promoción del ejercicio de la facultad de comprobación fiscal	89
Solicitud de aclaración	56
Promoción de responsabilidad administrativa sancionatoria	421
Pliego de observaciones	577
Denuncia de hechos	158
Fincamiento de responsabilidad resarcitoria	180

Nota: adaptado de ASF (2018).

Resultado de estas auditorías, la ASF reporta año tras año los montos económicos que han sido recuperados, denominados recuperaciones operadas, esto es, el reintegro al erario del Estado de los valores que fueron empleados de forma incorrecta (Sepúlveda, 2010). Existen, además, otros valores que se encuentran en proceso de recuperación o litigo. La tabla 5 muestra la tendencia ascendente de las recuperaciones operadas, que alcanzan la suma aproximada de MXN 141 millones, los que, por ejemplo, equivalen al 4 % de los 3433 millones de MXN desviados en el caso de la Estafa Maestra, antes descrito.

Tabla 5

Recuperaciones producto de la ejecución de las auditorías forenses (en millones de pesos mexicanos)

Año cuenta pública	Operadas
2009	13,2
2010	29,0
2011	17,1
2012	3,1
2013	11,6
2014	0,0
2015	0,0
2016	67,3
	141,3

Nota: tomado de ASF (2018).

5.2. El caso de Perú

Para atender las irregularidades que afectan los recursos públicos de este país interviene la CGR por medio del Departamento de Auditoría Forense (DFOR) o de la entidad que haga sus veces. El presunto cometimiento de un delito penal también es investigado de forma complementaria por el Ministerio Público (CGR, 2015). En Perú la auditoría forense es coordinada e instrumental y concluye con la elaboración del informe pericial. La CGR y el Ministerio Público ejecutan acciones conjuntas en la obtención de evidencias que sustenten dicho informe, puesto a disposición del fiscal responsable de la investigación una vez que finaliza las acciones de control (CGR, 2015).

Después de remitirse el informe pericial 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 (CGR, 2002). Sin embargo, se mantiene la reserva y secreto de la investigación en la instancia fiscal (CGR, 2015), en cumplimiento del numeral 1 del artículo 324 del Nuevo Código Procesal Penal (NCPP, 2004).

Aun cuando existe el sigilo de la información relacionada con los informes periciales forenses, dado que son de carácter reservado y no han sido publicados, en el año 2016 se realizó una encuesta a cuarenta y seis servidores públicos que desempeñan funciones administrativas financieras en 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 de modo afirmativo (Arohuanca, 2016), como se demuestra en la siguiente tabla:

Tabla 6

Necesidad de implementar auditoría forense

Ítem	Grupos sociales	Alternativas						Total	
		Sí	%	No	%	Otros	%	Cantidad	%
1.-	Funcionarios 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).

5.3. El caso de Ecuador

El 24 de mayo de 2012 se detectó en el Ministerio del Ambiente (MAE) el desvío de fondos públicos por 7 600 798,00 dólares transferidos de modo electrónico a terceros particulares mediante el uso del Sistema Integrado de Gestión Financiera (eSigef) (MAE, 2018). En otro caso ocurrido en abril de 2013, en el Gobierno Autónomo Descentralizado Municipal (GADM) del cantón Riobamba, se utilizó el Sistema de Pagos Interbancarios (SPI) del Banco Central del Ecuador (BCE) para desviar de modo electrónico 13 308 261,00 dólares 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). Ambos casos tienen en común la transferencia de valores monetarios por canales electrónicos oficiales.

Ante estos hechos, el MAE inició en mayo de 2012 un examen especial en el cual se analizaron las transferencias efectuadas a cuentas bancarias de terceros particulares que no tenían relación laboral ni contractual alguna con el citado ministerio. Los resultados de la auditoría revelaron que no fue posible identificar la dirección IP del dispositivo desde el cual se realizaron las transferencias, así como tampoco a las personas que realizaron las transacciones y los usuarios que manipularon las opciones del eSigef para crear en dicho sistema las cuentas beneficiarias (CGE, 2013).

Para el caso del GADM Riobamba, en abril de 2013 la CGE inició un examen especial para el análisis de operaciones, administración de identidades de cuentas de usuarios y monitoreo de transacciones electrónicas efectuadas mediante el Sistema de Pagos Interbancarios (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, en razón de que fueron incautados por la FGE. Tal como sucedió en el caso anterior, no fue posible identificar las direcciones IP del dispositivo desde el cual se efectuó la transacción como tampoco 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 analizados por la FGE, entidad que procesa en lo penal a los presuntos responsables, entre los cuales se encontró a un exfuncionario público del GADM. En este contexto, el exfiscal general del Estado 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, p. 18).

Es importante señalar que en los artículos del 19 al 23 de la Ley Orgánica de la Contraloría General del Estado (Locge) se describen las modalidades de auditoría que efectúa la CGE, siendo: 1) examen especial, que estudia aspectos limitados de las actividades realizadas en las entidades públicas con posterioridad a su ejecución; 2) auditoría financiera, que informa sobre la razonabilidad de las cifras constantes en los estados financieros de las entidades; 3) auditoría de gestión, que examina el control interno y la gestión realizada en la institución pública con base en indicadores de desempeño; 4) auditoría de aspectos ambientales, que audita aspectos de impacto ambiental; y 5) auditoría de obras públicas o de ingeniería, que evalúa la administración de las obras en construcción; sin que exista como modalidad la

auditoría forense y como parte de esta la informática forense, con técnicas que permitan el análisis, reconstrucción y validación de información, tales como observación, inspección, conciliación, preservación, recuperación, reconstrucción de archivos, entre otras, observando los estándares internaciones antes descritos.

6. Conclusiones

México y Perú 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, concluyendo de la comparación efectuada que, en esta materia, dichos países muestran un adelanto respecto del nuestro, experiencia que puede ser aprovechada por Ecuador en el desarrollo de políticas públicas que permitan ubicarnos a la vanguardia en el control de los recursos públicos, siendo el reto hacerlo a corto y mediano plazo y bajo los principios de eficacia, eficiencia y calidad.

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 admisible en lo posterior 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.

De esta manera, se concluye que otra de las técnicas de informática forense identificadas es la de localizar, recopilar y organizar información relevante almacenada de forma electrónica, inclusive, con el uso de programas informáticos especializados, si esta 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. 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 (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.

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, mediante la utilización de *software* especializado, con técnicas que permitan el análisis, reconstrucción y validación de información, tales como observación, inspección, conciliación, preservación, recuperación, reconstrucción de archivos, entre otras, observando los estándares internaciones ISO27037, RFC3227, UNE71505 y UNE71506, entre otros, 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 (Comisión Técnica Especial de Ética Pública, Probidad Administrativa y Transparencia [Cepat], 2005), en concordancia con lo establecido en el EGSI 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" (Secretaría Nacional de Administración Pública [SNAP], 2013), constituyéndose esta explicación en la respuesta a la interrogante planteada.

7. Referencias bibliográficas

Acurio, S. (10 de febrero de 2018). *Organización de los Estados Americanos.* Recuperado de 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 Nacional [AN] (2014). *Código Orgánico Integral Penal.* Quito: Publicado en el Suplemento del RO 180 de 10 de febrero del 2014.

Auditoría Superior de la Federación [ASF] (20 de julio de 2018). Recuperado de https://www.asf.gob.mx/

_____ (2017). *Manual de Organización de la ASF.* Ciudad de México.

Banco de México [Banxico] (11 de agosto de 2018). Recuperado de http://www.banxico.org.mx/

Banco Mundial (1 de agosto de 2018). Recuperado de http://www.bancomundial.org/

Cámara de Diputados (2016). *Ley de Fiscalización y Rendición de Cuentas de la Federación.* Ciudad de México.

_____ (2000). *Ley de Fiscalización Superior de la Federación.* Ciudad de México.

Canedo, A. (2010). La informática forense y los delitos informáticos. *Revista Pensamiento Americano*, 81-88.

Comisión Técnica Especial de Ética Pública, Probidad Administrativa y Transparencia [Cepat] (2005). *Auditoría forense, Herramienta de las EFS en la lucha contra la corrupción*. Quito.

Comunidad Andina [CA] (20 de julio de 2018). Recuperado de http://www.comunidadandina.org/

Contraloría General de la República [CGR] (2015). *Resolución de Contraloría N.º 373-2015-CG - Auditoría Forense*. Lima.

_____ (2004). *Nuevo Código Procesal Penal - Decreto Legislativo 957*. Lima.

_____ (2002). *Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República - Ley 27785*. Lima.

_____ (1929). *Decreto Supremo de 26 de septiembre de 1929*. Lima: DO El Peruano de 2 de octubre de 1929. Recuperado de http://www.contraloria.gob.pe/

Contraloría General del Estado [CGE] (2018). *Estatuto Orgánico de Gestión Organizacional por Procesos de la CGE*. Quito: Acuerdo 0003-CG-2018 de 19 de enero de 2018 publicado en el RO Edición Especial 244 de 26 de enero de 2018.

_____ (1 de diciembre de 2017). Recuperado de http://www.contraloria.gob.ec/LaInstitucion/Historia/HistoriaCGE

_____ (2013). *Informe General DAPAyF-0006-2013*. Quito: Informes aprobados CGE.

_____ (2013). *Informe General DATI-0002-2013*. Quito: Informes aprobados CGE.

_____ (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.

_____ (2002). *Ley Orgánica de la CGE*. Quito: Publicada en el Suplemento del RO 595 de 12 de junio de 2002.

_____ (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.

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.

Córdova, J., Correa, P., Echerri, F., & Pérez, J. (2017). Law versus Cybercrime. *Global Jurist*, 1-9.

Fiscalía General del Estado [FGE] (24 de julio de 2018). Recuperado de https://www.fiscalia.gob.ec/

Fonseca, O. (2007). *Auditoría gubernamental moderna*. Lima: Editorial IICO.

Guerra, C. (2014). *Análisis y aplicación de software para la recuperación forense de evidencia digital en dispositivos móviles Android*. Quito.

Gervilla, C. (2014). *Metodología para un análisis forense*. Cataluña: Repositorio Institucional de la Universidad Abierta de Cataluña.

González, J. (1995). *La imputabilidad en el derecho penal español*. Málaga: Comares.

Instituto de Altos Estudios Nacionales [IAEN] (10 de diciembre de 2017). Recuperado de http://www.iaen.edu.ec/lineas-de-investigacion/

López, O., Amaya, H., y 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.

Mark, K., & Chin, B. (2008). Computer forensics: from the technological, procedural/organisational and legal perspectives. *International Journal of Liability and Scientific Enquiry*, 335-350.

Márquez, R. (1992). *El tipo penal*. Ciudad de México: Universidad Nacional Autónoma de México.

Matthews, D. (2010). eDiscovery versus Computer Forensics. *Information Security Journal: A Global Perspective*, 118-123.

Mexicanos Contra la Corrupción y la Impunidad [MCCI] (27 de diciembre de 2018). *La estafa maestra: graduados en desaparecer dinero público*. Recuperado de https://www.animalpolitico.com/estafa-maestra/

_____ (28 de diciembre de 2018). *ASF interpone 7 denuncias contra Sedatu y Sedesol por presuntos desvíos*. Recuperado de https://www.animalpolitico.com/2018/10/estafa-maestra-auditoria-denuncias-sedatu-sedesol/

Ministerio del Ambiente [MAE] (25 de dicimbre de 2018). Recuperado de http://www.ambiente.gob.ec/el-ministerio-del-ambiente-mae-informa-en-torno-al-caso-del-desvio-de-fondos-3/

Ministerio de Telecomunicaciones y de la Sociedad de la Información [Mintel] (2016). *Plan Nacional de Telecomunicaciones y Tecnologias de Informacion 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*. Ciudad de México: Pearson Educación.

Organización de los Estados Americanos [OEA] (2013). *Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos*. Washington, D. C.

Organización Internacional de Entidades Fiscalizadoras Superiores [Intosai]. (10 de agosto de 2018). Recuperado de www.intosai.org.

Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores [Olacefs] (19 de diciembre de 2017). Recuperado de http://www.olacefs.com.

_____ (2012). La auditoría forense fortalece el trabajo de las EFS. *Olaacefs*, 18.

Pardo, L. (2011). Aplicación de las nuevas tecnologías en la administración pública. *Revista de Contabilidad y Dirección*, 105-126.

Secretaría Nacional de Administración Pública [SNAP] (2015). *Plan Nacional de Gobierno Electrónico 2014-2017*. Quito.

_____ (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.

Secretaría Nacional de Planificación y Desarrollo [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.

Servicio Nacional de Medicina Legal y Ciencias Forenses [SNMLCF] (10 de febrero de 2018). Recuperado de https://www.cienciasforenses.gob.ec/mision-vision/

_____ (20 de julio de 2018). Recuperado de https://www.cienciasforenses.gob.ec/servicios-de-criminalistica/

_____ (2017). *Estatuto Orgánico*. Quito.

_____ (2015). *Decreto Ejecutivo 759 de 27 de agosto de 2015*. Quito: Publicado en el RO Suplemento 585 de 11 de septiembre de 2015.

Villardefrancos, M. d., y 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.

Zambrano, A. (2009). *Manual de práctica procesal penal*. Perú: ARA Editores E. I. R. L.

Zárate, A., y Eleuterio, G. (2019). *Derecho penal parte general*. Madrid: Editorial Universitaria Ramón Areces.