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

SITUACIÓN DE LA AUDITORÍA DE DELITOS INFORMÁTICOS EN EL SECTOR PÚBLICO ECUATORIANO

Autor: Adriana Yolanda Fuentes Arteaga
Director: Romel AlfredoTintín Hidalgo

Quito, mayo, 2019.

INSTITUTO DE ALTOS ESTUDIOS NACIONALES
LA UNIVERSIDAD DE POSGRADO DEL ESTADO

No.216- 2019.

ACTA DE GRADO

En el Distrito Metopolitano de Quito, hoy a los nueve días del mes de mayo del año dos mil diecinueve, **ADRIANA YOLANDA FUENTES ARTEAGA,** portadora del número de cédula: 0401219860, **EGRESADA DE LA MAESTRÍA EN AUDITORIA GUBERNAMENTAL Y CONTROL (2016-2018),** se presentó a la exposición y defensa oral de su Artículo Científico, con el tema: **"SITUACIÓN DE LA AUDITORÍA DE DELITOS INFORMÁTICOS EN EL SECTOR PÚBLICO ECUATORIANO",** 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:	9.38
Artículo Científico Escrito:	8.50
Defensa Oral Artículo Científico:	9.20
Nota Final Promedio:	**9.11**

INSTITUTO DE ALTOS ESTUDIOS NACIONALES
LA UNIVERSIDAD DE POSGRADO DEL ESTADO
SECRETARÍA GENERAL

En consecuencia, **ADRIANA YOLANDA FUENTES ARTEAGA,** se ha hecho acreedora al título mencionado.

Para constancia firman:

Mgs. Ana Ponce.
PRESIDENTE Y MIEMBRO DEL TRIBUNAL

Mgs. Grace Tamayo.
MIEMBRO

Abg. Ximena Carvajal Chiriboga.
DIRECTORA DE SECRETARÍA GENERAL

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

Fojas 1/1

Fecha 14 JUN 2019

Secretaría General

INSTITUTO DE ALTOS ESTUDIOS NACIONALES
LA UNIVERSIDAD DE POSGRADO DEL ESTADO

AUTORÍA

Yo, Adriana Yolanda Fuentes Arteaga, máster, con CC 0401219860 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 de la autora del trabajo de titulación. Asimismo, me acojo a los reglamentos internos de la universidad correspondientes a los temas de honestidad académica.

Adriana Fuentes

Firma

CC.: 0401219860

INSTITUTO DE ALTOS ESTUDIOS NACIONALES
LA UNIVERSIDAD DE POSGRADO DEL ESTADO

AUTORIZACIÓN DE PUBLICACIÓN

Autorizo al Instituto de Altos Estudios Nacionales (IAEN) la publicación de este artículo científico, de su bibliografía y anexos, como artículo en publicaciones para lectura seleccionada o fuente de investigación, siempre dando a conocer el nombre del autor y respetando la propiedad intelectual del mismo.

Quito, mayo, 2019.

Adriana Fuentes

FIRMA DEL EGRESADO

ADRIANA YOLANDA FUENTES ARTEAGA

NOMBRE DEL EGRESADO
CC.: 0401219860

SITUACIÓN DE LA AUDITORÍA DE DELITOS INFORMÁTICOS EN EL SECTOR PÚBLICO ECUATORIANO

Autor: Adriana Yolanda Fuentes Arteaga

Resumen

El artículo analiza ¿por qué la Contraloría General del Estado en las auditorías ejecutadas en el ámbito de la Administración Pública, ha considerado a las acciones ilícitas realizadas con herramientas informáticas como: delitos de peculado, cohecho, concusión y enriquecimiento ilícito y no como delitos informáticos?

Esté artículo compara cualitativamente la normativa vigente con la internacional, define el nivel de conocimiento en delitos informáticos, normativa y las debilidades en herramientas informáticas en la Contraloría General del Estado mediante 30 encuestas; y, analiza cuantitativamente 24 casos de denuncias en delitos con el uso de las Tecnologías de Información y Comunicación (TICs) en Ecuador y su relación con 2214 informes de indicios de responsabilidad penal e informes generales realizados por la Contraloría General del Estado.

El artículo determina que la Contraloría General del Estado en las acciones de control realizadas a entidades públicas en donde existió delitos con el uso de TICs y que se relacionan con los delitos informáticos tipificados en el Código Orgánico Integral Penal (COIP, 2014), emitió informes con indicios de responsabilidad en delitos en contra de la administración pública y no como delitos informáticos. En la normativa actual del COIP, las sanciones establecidas en los delitos en contra de la administración pública son altas en comparación a los delitos informáticos. Se recomienda actualizar esta normativa.

Summary

The article analyzes why the Comptroller General of the State in audits performed in the field of Public Administration, has considered illicit actions carried out with computer tools such as: embezzlement´s crimes, bribery, concussion and enrichment and not as computer crimes?

This article will compare qualitatively the current regulationswith the international, defines the level of knowlegde in computer crimes, regulations and weaknesses in computer tools in the Comptroller's Office through 30 surveys; and, it analyzes quantitatively 24 cases of denunciations in crimes with the use of Information and Communication Technologies (ICTs) in Ecuador and its relationship with 2 214 reports of criminal liability and general reports made by the Comptroller General of the State.

The article determines that the General Comptroller of the State in the control acticarried out to public entities where there were crimes with the use of ICTs and that are related to the computer crimes typified in the COIP (Organic Comprehensive Criminal Code, COIP, 2014), issued reports with indications of responsibility in crimes against the public administration and not as computer crimes. In the current COIP regulations, the sanctions established in crimes against the public administration are high compared to computer crimes. It is recommended to update this normative.

Palabras Claves: Delitos informáticos, era de la información, hábitat delictivo, ciberespacio, bugs y ciberdelincuencia.

Introducción

En el siglo XXI con el desarrollo informático nace una sociedad moderna que usa la tecnología juntamente con el internet y las redes sociales revolucionando la vida del ser humano; el abuso de la tecnología ha causado que la información se convierta en una herramienta empleada en algún comportamiento ilícito que afecta a los bienes, sistemas de información, entre otros, dando surgimiento a la existencia de la ciberdelincuencia como una modalidad de actuación criminal, establecido en la normativa penal (Colás, 2016).

Según el Observatorio Latinoamericano de Delitos Informáticos establecido en Argentina durante los años 2014 a 2017 en Latinoamérica se han registrado en este sitio 2760 denuncias sobre delitos informáticos de los cuales el 2,27% se realizaron en Ecuador, el 3,21% de los registros corresponde a víctimas en organismos gubernamentales correspondiente a datos de 21 países (ODILA, 2017). Por lo que es importante analizar las casusas de los delitos informáticos y como estas son directamente proporcional a los adelantos de las tecnologías de información (Loredo y Ramírez, 2013). También es indispensable establecer regulaciones jurídicas relacionadas y actualizadas con los avances tecnológicos, considerando que la tecnología permite realizar acciones no establecidas en la ley, cometiendo delitos tradicionales como robo, fraude, chantaje y falsificación, en delitos informáticos o computacionales, los que tienen la capacidad de cometer un acto ilegal desde cualquier lugar del mundo, con gran acceso informático, a más de la ventaja del anonimato (Gonzáles, Bermeo, Villacreses, y Guerrero, 2018).

El Plan Nacional Para el Buen Vivir 2013 - 2017, publicado en el registro oficial suplemento 78 de 11 de septiembre del 2013 y modificado el 13 de julio de 2015, menciona que Ecuador tuvo una inversión en ciencia y tecnología entre los años 2007 a 2010, con un incremento histórico del 108% en relación al Producto Interno Bruto (PIB), y el Instituto Nacional de

Estadísticas y Censos en el informe Módulo de Tecnologías de la Información y Comunicación TIC de las Encuestas de Manufactura y Minería, Comercio Interno y Servicios detalla que en los años 2015 a 2016, el Ecuador se ubica en el puesto 83 en el uso de Tecnologías de Información y Comunicación TIC, por encima de Bolivia, Perú, y por debajo de Colombia entre los países del CAN, por lo que el país debe considerar que la falta de seguridad en los sistemas de información, el almacenamiento de información en el internet, el desconocimiento de medidas de prevención en uso de claves, el uso de software pirata, entre otros, permiten que una organización se encuentre vulnerable, facilitando el acceso a la confidencialidad de la información, a los datos, a los sistemas, entre otros; relacionados al contenido de la propiedad intelectual y a los derechos afines e informáticos, confirmando lo mencionado por Pons (2017) que afirma. “El robo o pérdida de material sensible, también se considera como una amenaza que afecta a la fuga de datos y robos de identidad” (p.6).

La Dirección de Política Criminal de la Fiscalía General del Estado registro los siguientes casos por denuncias delitos informáticos durante los siguientes años: 2010 registro 1099 casos, 2011 registro 3129 casos, 2012 registro 2682 casos, 2013 registro 2070 casos, 2014 registro 877 casos y 2015 registro 626 denuncias hasta el 31 de mayo. En estos datos estadísticos se observa que existía un número elevado de denuncias antes del 10 de agosto de 2014, fecha en la cual entro en vigencia el Código Orgánico Integral Penal.

En las estadísticas proporcionadas por la Fiscalía General del Estado no es posible establecer el número de delitos relacionados con la Administración Pública, sin embargo en la base de datos publicada por la Contraloría General del Estado durante los años 2004 a 2017 se remitieron 2214 informes con indicios de responsabilidad penal a la Fiscalía General del Estado, por lo que el objetivo fundamental de este trabajo es observar algunos informes realizados por la Contraloría

General del Estado, mediante el análisis de la redacción de comentarios, la aplicación de la normativa nacional e internacional referente a delitos informáticos o cometidos con el uso de Tecnologías de Información y Comunicación (TICs), considerando que en la actualidad el Ecuador en su legislación cuenta con leyes y normas que sancionan los delitos informáticos en derecho penal, derecho procesal y en cooperación internacional.

De ahí la importancia de conocer si la Contraloría General del Estado, al ser el principal regulador del Sistema de Control, Fiscalización y Auditoría, y aplicar los principios constitucionales, especialmente de legalidad, responsabilidad financiera, transparencia, economía, eficiencia y eficacia, junto con los criterios de equidad, ética y las políticas de descentralización y desconcentración en la administración pública, que dispone de normas, guías, procedimientos e instrumentos de auditoría (programas, herramientas de ofimática, etc.), según la Ley Organica de la Contraloría General del Estado (LOCGE, 2015). Esta entidad mantiene estos instrumentos actualizados y acordes con estándares internacionales; lo que permitirá obtener un análisis forense digital y eficiente; proponiendo posibles soluciones en la ejecución de auditorías informáticas forenses.

Instrumentos legales en delitos informáticos

En la administración pública con la aparición de las nuevas Tecnologías de la Información y Comunicación (TICs), los sistemas de información están relacionados en forma transversal con todas las actividades de las entidades, por lo que al realizar una auditoría informática o auditoría de TI es importante considerar a Mora (2017) que afirma. “La auditoría informática es un proceso en evolución, ya que cada vez hay nuevos riesgos asociados a la materialización sobre la tecnología que está en constante movimiento; que también es cambiante e innovadora” (p.8).
La Ley Organica de la Contraloría General del Estado clasifica a la auditoría gubernamental en

los siguientes modalidades: 19 Examen especial, 20 Auditoría financiera, 21 Auditoría de gestión, 22 Auditoría de aspectos ambientales y 23 Auditoría de obras públicas o de ingeniería.

Es importante mencionar que a pesar de esta clasificación los procesos de una auditoría informática o auditoría TI se deben aplicar a todos los tipos de auditoría considerando lo establecido por la Organización Internacional de las Entidades Fiscalizadoras Superiores (INTOSAI, s.f.). En las Directrices sobre auditoría de TI en la cual menciona lo siguiente:

Auditoría de TI es, por lo tanto, un término amplio que abarca las auditorías financieras (para evaluar la exactitud y el cumplimiento de las manifestaciones realizadas en los estados financieros de una organización), las auditorías de cumplimiento (evaluación de los controles internos); y, las auditorías operativas (para evaluar si los sistemas de TI satisfacen las necesidades de los usuarios y no someten a la entidad a riesgos innecesarios). Sin embargo, puede haber casos en que algunas auditorías sólo se destinen a evaluar un determinado componente TI de un sistema.

(ISSAI 5300, 2016, p.3)

Es necesario aplicar las Normas de Control Interno (NCI, 2009), emitidas mediante Acuerdo 039-CG de 16 de noviembre de 2009, publicado en Registro Oficial 78 de 1 de diciembre de 2009 aplicables en todas las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, las cuales están conformadas en seis grupos de acuerdo al siguiente detalle: 100-00 Normas Generales, 200-00 Ambiente de Control, 300-00 Evaluación del Riesgo, 400-00 Actividades de Control, 500-00 Información y Comunicación; y, 600-00 Seguimiento. Madariaga (2004) menciona que la evaluación de control interno es indispensable en los sistemas de información a pesar de la efectividad de actividades y funciones.

Palíz (2017) señala que las Normas de Control Interno relacionadas a las TI están incompletas en comparación a estándares internacionales, lo que afectaría determinar una planificación de la auditoría basada en los riesgos como lo establece la ISSAI.

Según lo establecido en las Normas Ecuatorianas de Auditoría Gubernamental (NEAG, 2015) AG–05 relacionadas con el auditor gubernamental participación de profesionales y/o especialistas en la auditoría gubernamental, los equipos de auditoría pueden ser multidisciplinarios es decir intervienen profesionales de diversas disciplinas como: contadores, abogados, investigadores informáticos, entre otros, los cuales cumplen con el análisis de los sistemas de información que intervienen en todas las áreas.

Una de las herramientas que permite la detección y verificación de delitos informáticos o tecnológicos es la técnica de la auditoría forense (Cáceres y De La Torre, 2017). Refiriéndose a los procedimientos de auditoría que tienen términos forenses como evidencias y pruebas penales.

La Constitución de la República del Ecuador del 2008, en el artículo 212, numeral 2, dispone, entre las funciones de la Contraloría General del Estado, la de determinar indicios de responsabilidad penal, sin perjuicio de las funciones que en esa materia tiene la Fiscalía General del Estado. La Ley Orgánica de la Contraloría General del Estado, en el artículo 31, numeral 34, ratifica la capacidad de la Contraloría para determinar dichos indicios.

El Código Orgánico Integral Penal aprobado el 10 de agosto de 2014, en el artículo 581, numeral 2, establece, entre las formas de conocer la infracción penal el informe de supervisión que lo realizan los órganos de control y es remitido a la Fiscalía, sin perjuicio de lo que establece el ultimo inciso Ibídem, en el cual nos aclara que la Contraloría informará no solo en delitos de peculado y enriquecimiento ilícito como presupuesto de prosedibilidad, sino que es un deber del

órgano de control informar a la Fiscalía de cualquier anomalía que se encuentre dentro de una acción de control que afecte a los recursos públicos.

Por lo que considerando lo mencionado la Contraloría General del Estado dentro de sus funciones puede establecer los siguientes delitos tipificados en el COIP en relación a los delitos informáticos.

Tabla 1

Delitos informáticos tipificados en el COIP y su sanción.

Tipo	Sanción
Artículo 190.- Apropiación fraudulenta por medios electrónicos.	1 a 3 años
Artículo 229.- Revelación ilegal de base de datos.	3 a 5 años
Artículo 230.- Interceptación ilegal de datos.	3 a 5 años
Artículo 231.- Transferencia electrónica de activo patrimonial.	3 a 5 años
Artículo 232.- Ataque a la integridad de sistemas informáticos.	3 a 5 años
En bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana.	5 a 7 años
Artículo 233.- Delitos contra la información pública reservada legalmente.	5 a 7 años
Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	3 a 5 años

Nota. Fuente: Código Organico Integral Penal

Es importante mencionar que en el artículo 233 de la Constitución de la República, los delitos en contra de la Administración Pública, son los siguientes:

Tabla 2

Delitos en contra de la administración pública tipificados en el COIP y su sanción.

Tipo	Sanción
Artículo 278.- Peculado	
Quienes abusen, se apropien, distraigan o dispongan arbitrariamente de recursos públicos.	10 a 13 años
Utilicen trabajadores remunerados por el Estado o por las entidades del sector público o bienes del sector público.	5 a 7 amos
Se aprovechen económicamente, en beneficio propio o de terceras personas, de estudios, proyectos, informes, resoluciones y más documentos.	5 a 7 años
Artículo 279.- Enriquecimiento ilícito (SBU: Salario Básico Unificado del Trabajado en General)	

Superior a 400 SBU.	7 a 10 años
Superior a 200 y menor a 400 SBU.	5 a 7 años
Hasta 200 SBU.	3 a 5 años
Artículo 280.- Cohecho	
Por recibir beneficios.	1 a 3 años
Por ejecutar el acto o no realizar el acto debido.	3 a 5 años
El acto sirvió para cometer otro delito.	5 a 7 años
Artículo 281.- Concusión	
Por exigir derechos, cuotas, entre otros.	3 a 5 años
Se realizó con amenazas o violencia.	5 a 7 años

Nota. Fuente: Código Organico Integral Penal

Delitos informáticos en las organizaciones públicas en Ecuador

En la actualidad con los avances tecnológicos y de los sistemas de información se ha producido un crecimiento importante en el factor económico, social y cultural de los países; sin embargo, existen evidencias del acceso a los sistemas de información lo que ha permitido el aumento de sucesos criminales (Villamizar, Orjuela y Adarme, 2015). Por lo que las entidades del estado que usan Tecnologías de Información y Comunicaciones (TICs) durante la ejecución de sus procesos forman parte de esta era y están vulnerables a ataques y amenazas denominados delitos informáticos. Concordando con lo mencionado por Arias y Domingos (2016) que afirman. “Según avanzó la Informática y su aplicación en el campo económico, se desencadenaron los aspectos nocivos, relacionados con el delito informático” (p.64).

Lo que nos conduce a realizar un control a los sistemas de información dando paso a una auditoría informática o forense, considerando lo que menciona Pons (2017) que afirma. “Con la aparición del ciberespacio, el hábitat delictivo ha crecido exponencialmente, pues la era de la información multiplica las oportunidades de los delincuentes” (p.13). Y, esto comprende a un aumento considerable en la determinación de responsabilidades: administrativa culposa, civil culposa e indicios de responsabilidad penal relacionados a delitos informáticos.

En tal sentido la Informática no es ajena al campo de la Auditoría, posibilitándole a los auditores encargados de revisar y evaluar los controles contables, activos y patrimonio de la organización, no solo rapidez y eficacia, sino también que al aplicar las tecnologías de la información en las auditorías, se ha obligado a esta a responder con alternativas, a las críticas y cuestionamientos realizados por autoridades e inversionistas, sobre la necesidad y conveniencia de investigar si los principios y normas para la revisión de los sistemas computarizados empleados por los auditores, aún conservan toda su validez y responden a los objetivos de esta ciencia.

(Arias y Domingos, 2016, p.59)

Al respecto, según la base de datos de informes remitidos a la Fiscalía General del Estado ubicada en la página web de la Contraloría General del Estado de los años 2004 al 2017 con un total de 2214 registros no existen informes con indicios de responsabilidad penal en delitos informáticos o computacionales, como se demuestra en la tabla siguiente:

Tabla 3

Informes de la Contraloría General del estado remitidos a la Fiscalía, de todo el país.

INFORMES REMITIDOS A LA FISCALÍA	**AÑOS**															
DELITO	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**S/A**	**TOTAL**
ABUSO DE CONFIANZA								1								1
CONCUSION								1								1
DEFRAUDACION ADUANERA		1													1	2
ENRIQUECIMIENTO ILICITO			1	1	2	8	13	21	5	10	2	11	21	5	2	102
FALSIFICACION DE DOCUMENTOS		24	3	3	12	25	2	4	2	1	1			1	5	83
NEPOTISMO											1					1
PECULADO	2	6	16	118	259	323	132	125	179	188	83	311	233	2	42	2019
TERMINADO						1										1
TRAFICO DE INFLUENCIAS													1	2		3
USURPACION DE FUNCIONES				1												1
TOTAL	**2**	**31**	**20**	**123**	**273**	**357**	**147**	**152**	**186**	**199**	**87**	**322**	**255**	***10**	**50**	**2214**

Nota. Fuente: Página Web de la Contraloría General del Estado

*En este año la base de datos no ha sido actualizada

Confirmando que el 91% de informes son de peculado, el 5% de enriquecimiento ilícito y el 4% de falsificación de documentos.

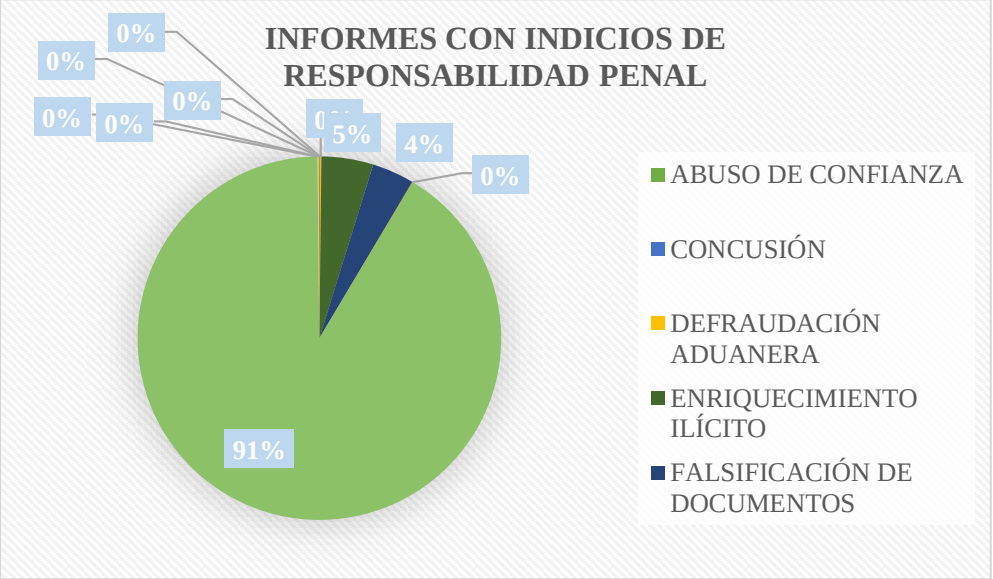

Figura 1. Porcentaje por tipos de delitos enviados a la Fiscalía. Fuente: Página Web de la Contraloría General del Estado.

De algunos reportes de prensa difundidos en internet se observaron 24 casos de delitos realizados con el uso de TICs durante los años 2010 al 2017, a los que según descripción del delito se los clasificó de acuerdo a las siguientes características:

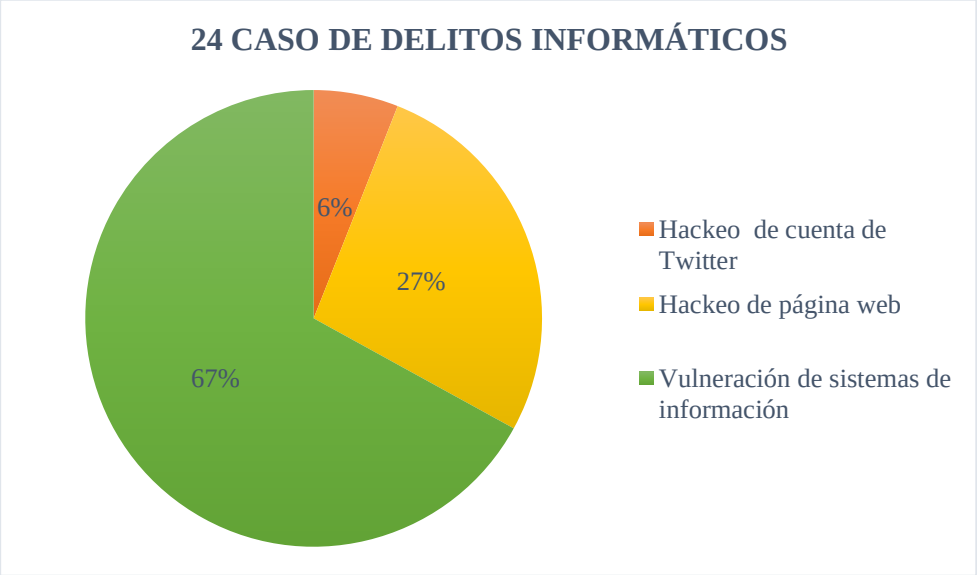

Figura 2. Casos de tipos de delitos en Ecuador. Fuente: Páginas de diarios en internet.

Además, se constató que, de los 24 casos, 11 de estos se encuentran relacionados con informes generales de auditoría publicados en la página web de la Contraloría General del Estado; sin embargo, únicamente 7 casos se encuentran vinculados a la base de datos de informes enviados a la Fiscalía con delito de peculado.

Al realizar un análisis de las denuncias de los delitos publicados en la prensa por internet, y los comentarios de los informes se constató que los delitos están relacionados con el uso de TICs, concordando con Alcívar, Blanc, y Calderón (2018) que afirman. "Los delitos informáticos son los que utilizan medios informáticos como por ejemplo la utilización de una computadora conectada a una red bancaria, para cometer delitos tradicionales como una estafa, robo, o hurto, también se considera como delito computacional"(p.3).

Existen varios casos de delitos computacionales; sin embargo, se detallan algunos a continuación:

Caso Hospital General Provincial Luis G. Dávila: El número de informe con indicios de responsabilidad penal remitido a la Fiscalía fue DR7-DPC-AE-0021-2015 con delito de peculado; y, el informe general publicado en la página web de la Contraloría DR7-DPC-AE-0001-2016[1], en este último se puede verificar en el comentario "Transferencias bancarias por adquisiciones de bienes o servicios sin que se evidencie la correspondiente contraprestación", que el delito fue cometido con el uso de un sistema de información denominado eSlGEF implementado por el Ministerio de Finanzas, en el que se realizaron desembolsos, con un total de 170 CUR y 172 transferencias bancarias realizadas a cuentas particulares, sumando un total

[1] Informe de Examen especial a los ingresos; gastos, procedimiento precontractual de subasta inversa electrónica de bienes SIE-HLGD--041-2013 y denuncia de los procesos de adquisición, distribución de medicamentos y atención al usuario del Hospital General Provincial Luis G. Dávila. Período desde: 2009/01/01 hasta: 2014/12/31

de 713100,53 USD., los cuales no contaban con documentación de respaldo que evidencie la legalidad, propiedad y veracidad del gasto, respecto a los pagos efectuados.

Caso Dirección Distrital 04D01 San Pedro de Huaca - Tulcán - Educación: El informe con indicios de responsabilidad penal remitido a la Fiscalía con número DR7-DPC-AE-0010-2016[2] con delito de peculado, y DR7-DPC-AE-0012-2016 informe general publicado en la página web de la Contraloría, por lo que al verificar en este se constató que el comentario "Proceso de contratación RE-DESHT-001-2014 para el diseño e implementación de red en la Dirección Distrital, en el numeral 6, Uso de la clave del Sistema de Contratación Pública", es un delito cometido con el uso del sistema oficial de contratación pública SERCOP, en el que se refleja que el usuario en el proceso de contratación, no fue usado por la persona a la que fue asignada la clave porque existen evidencias que la misma fue proporcionada a la máxima autoridad, adicional también en el comentario se observa que todas las etapas del proceso de contratación fueron realizadas en un mismo día, sin mantener en el sistema ninguna restricción, por lo que este delito podría considerarse como informático al ser realizado como el uso de TICS.

Estos delitos por las características que mantienen al usar las TICs puede ser juzgado como delito informático, considerando que existen empleados o personas que usan sus conocimientos para su propio beneficio económico (Arias y Domingos, 2016).

Los datos estadísticos analizados concuerdan con Gonzáles, Bermeo, Villacreses, y Guerrero (2018) que afirman. "La criminalidad informática tiene un alcance mayor y puede incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados como medio" (p.3).

[2] Informe de Examen especial a los ingresos, gastos, procedimientos de contratación, adquisición, recepción y utilización de bienes y prestación de servicios y consultoría; y al proceso de cierre financiero, contable, presupuestario, nómina y bienes de la Dirección de Educación Hispana del Carchi. Período desde: 2011/01/03 hasta: 2016/03/31

Nivel de experiencia y conocimiento en delitos informáticos

En el sistema de control y fiscalización de la administración pública es imprescindible que existan personas que posean conocimientos y habilidades en el ámbito tecnológico y en auditoría informática forense, concordando con Mora (2017) afirma. “El personal auditor informático requiere de competencia especializada en la función informática, conocimientos de auditoría y de gestión empresarial” (p.2).

Para establecer el nivel de conocimiento en el área de auditoría informática forense y delitos informáticos en relación a la normativa establecida por la Contraloría General del Estado y la del país, se diseñó una encuesta enfocada al nivel de conceptos, normativa, herramientas y experiencias.

La encuesta se aplicó a 30 funcionarios públicos entre auditores en tecnología de la información, personal de apoyo tecnológico e ingenieros informáticos de entidades públicas, lo que permitió detectar lo siguiente:

Tabla 4

Resultado de encuesta a auditores informáticas e ingenieros en sistemas.

Conocimientos	**Porcentaje**
En delitos informáticos.	100,0%
En normativa penal relacionada a delitos informáticos.	86,2%
En normativa de la CGE en relación con estándares internacionales.	34,5%
Informes de auditoría de la CGE con indicios de responsabilidad penal relacionados a delitos informáticos.	20,7%
En auditoría informática forense.	72,4%
En herramientas tecnológicas usadas por la CGE.	13,8%
Seguridad informática.	96,6%

Nota. Fuente: Encuestas realizadas por autor a 30 ingenieros informáticos.

Este instrumento reveló elementos claves en el nivel de conocimiento en cuanto a que los auditores informáticos e ingenieros informáticos tienen un nivel alto de conocimientos en delitos

informáticos (100%) y seguridad informática (96,6%), mientras que en la normativa aplicarse el nivel es bajo (86,2% y 34,5%), por lo que no se estaría aplicando lo siguiente:

El auditor de sistemas debe mantenerse actualizado, ampliando sus conocimientos a tiempo presente, en lo concerniente a técnica o metodología de Auditoría Informática, gestión, planificación y organización de las tecnologías de información, infraestructura técnica, protección de activos informáticos, planes de contingencias y de continuidad de los procesos del negocio soportados por los sistemas de información, verificación del cumplimiento de controles internos, normativas y procedimientos establecidos por la gerencia para los sistemas informáticos, entre otros; ya que vendrán los retos, que se deben atender de acuerdo a las tendencias del presente siglo, es algo ineludible para su profesión.

(Mora Q, 2017, pág. 11)

Es importante mencionar que el nivel de desconocimiento en herramientas informáticas es bajo (13,8%) por lo que no se estaría cumpliendo lo mencionado por Ocampo, Trejos, y Solarte (2010) que afirman. “El personal que trabaje en la informática forense deberá poseer sólidos conocimientos técnicos y prácticos y conocer las herramientas de uso, estar al día en bugs (vulnerabilidades) del sistema (sistemas operativos, software y hardware)” (p.4).

Los ejes temáticos aplicados en la encuesta de nivel de conocimientos en delitos informáticos, aplicación de la normativa y prácticas en técnicas de auditoría forense, también permitieron determinar algunos casos de delitos informáticos que se han producido en las entidades públicas, aportando a la base de conocimientos de este artículo.

En las entrevistas realizadas mediante un cuestionario a un Experto Supervisor de Auditoría de Tecnología de la Información y a un Especialista de Auditoría de Tecnología de la Información de la Contraloría General del Estado, se pudo determinar que la disminución de

riesgos de delitos informáticos no depende únicamente de actualizar la normativa o usar herramientas tecnológicas actualizadas sino de implementar controles de seguridad informática mediante el monitoreo periódico en todas las aplicaciones utilizadas por los usuarios, coincidiendo con Montoya (2009) que afirma. “Uno de los objetivos principales de establecer una política de seguridad es el de reducir al mínimo los riesgos posibles, implementando adecuadamente las diferentes medidas de seguridad” (p.4).

Con respecto a la experiencia, las entrevistas permitieron determinar que los auditores si tienen un amplio conocimiento en cuanto a conceptos, técnicas y normativa de juzgamientos, lo que garantiza que las actividades ejecutadas por el auditor se realicen con eficacia, considerando los estándares internacionales a través de las Normas Internacionales de Auditoria (NIA) y las Normas Internacionales de Aseguramiento de la Información (Gómez, 2014).

Sin embargo, es importante considerar que existen otras instituciones que contrarrestan los delitos informáticos como el Consejo de la Judicatura, la Fiscalía General del Estado; y, la Agencia de Regulación y Control de las Telecomunicaciones, por lo que el nivel de conocimiento del personal de estas entidades también aporta a la labor realizada por la Contraloría General del Estado concordando con Gonzáles, Bermeo, Villacreses, y Guerrero (2018) que afirman. “En el Ecuador las investigaciones realizadas acerca de pericia informática son de bajo interés, una de las causas es el desconocimiento del tema por parte de la sociedad, adicional a la falta de procedimientos registrados de delitos informáticos competentes a las autoridades o entidades gubernamentales” (p.4). Un ejemplo claro de esto son las estadísticas de peritos acreditados por el Consejo de la Judicatura en ingeniería informática o de sistemas para el período comprendido entre los años 2017 al 2021, que demuestran que existe únicamente 95 peritos informáticos en todo el país.

Tabla 5

Reporte del Consejo de la Judicatura de peritos acreditados por provincia en Ingeniería Informantica o de Sistema.

Provincia	**Peritos Acreditados**
AZUAY	15
CHIMBORAZO	5
COTOPAXI	3
EL ORO	3
ESMERALDAS	1
GALÁPAGOS	1
GUAYAS	13
IMBABURA	3
LOJA	2
LOS RÍOS	1
MANABÍ	4
NAPO	1
PASTAZA	1
PICHINCHA	32
SANTO DOMINGO TSACHILAS	3
TUNGURAHUA	7
Total	**95**

Nota. Fuente: Página Web del Consejo de la Judicatura

Como resultado del análisis efectuado en cuanto al nivel de conocimiento y experiencia, la Contraloría General del Estado y las entidades fiscalizadoras deben incorporar personal especializado considerando que Ecuador carece de profesionales en pericia informática con conocimientos adecuados, lo que permite la impunidad de casos (Gonzáles, Bermeo, Villacreses, y Guerrero, 2018).

Metodología

El artículo se realizó en forma cuantitativa y cualitativa, utilizando los métodos de análisis de datos, revisión documental, entrevistas y encuestas, con la finalidad de analizar las acciones de la Contraloría General del Estado en los delitos informáticos contra la administración pública.

El análisis de datos se realizó mediante tablas dinámicas y gráficos en Excel en los que se usó las siguientes bases de datos: informes de la Contraloría General del Estado remitidos a la Fiscalía de los años 2004 al 2017, con un total de 2214 registros, reportes de prensa difundidos en internet durante los años 2010 al 2017, con 24 casos y Reporte del Consejo de la Judicatura con 95 peritos acreditados en ingeniería informática o de sistemas para el período comprendido entre el 2017 al 2021, lo que permitió obtener un informe de entidades públicas con denuncias de delitos informáticos y las acciones que realizo la Contraloría General del Estado.

La revisión documental se efectuó mediante la recopilación y análisis de la normativa legal vigente sobre el proceso de auditoría en relación a tecnología como son: Constitución de la República del Ecuador, Código Integral Penal, Ley Orgánica de la Contraloría General del Estado, Normas de Control Interno, Acuerdos emitidos por la Contraloría, Directrices sobre auditoría de TI de la Organización Internacional de las Entidades Fiscalizadoras Superiores INTOSAI, lo que permitió comprender el marco legal vigente y determinar que es necesario que las Normas de Control Interno que se aplican en todas las entidades del estado, durante la implementación y evaluación del sistema de control interno, deben perfeccionarse con la incorporación de técnicas actualizadas (estándares internacionales) relacionadas con la seguridad informática en sistemas de información, características, tipos, sujetos y bien jurídico protegido; así como también, es necesario que la entidad de control incremente dentro de sus modalidades las auditorías de tecnologías con la aplicación de técnicas de auditoría forense.

Las entrevistas se aplicaron mediante cuestionarios a un Experto Supervisor de Auditoría de Tecnología de la Información y a un Especialista de Auditoría de Tecnología de la Información, con la finalidad de determinar el nivel de conocimiento en Auditorias Informáticas Forenses

relacionadas con delitos informáticos, permitiendo determinar que el personal de la Contraloría si tiene un nivel alto en conceptos, técnicas y normativa relacionados a delitos informáticos.

Las encuestas se realizaron a 30 personas en forma digital mediante formularios de Google entre los que se encontraba personal de apoyo tecnológico y técnicos de la Contraloría General del Estado, técnicos y usuarios de entidades públicas; es así, que el objeto de la encuesta se enfocó a determinar los niveles de conocimientos en delitos informáticos, aplicación de la normativa y prácticas en técnicas de auditoría forense, revelando que los niveles de conocimiento en delitos informáticos y en seguridad informática son altos; y, los niveles de conocimiento en normativa y herramientas informáticas son bajos.

Conclusiones:

En el análisis cualitativo de las normativas vigentes en el Ecuador y en la Contraloría General del Estado con los estándares internacionales, relacionados con los tipos de auditoría gubernamental fue posible determinar que el ente de control debe aplicar auditorías de TI como lo menciona la Organización Internacional de las Entidades Fiscalizadoras Superiores (INTOSAI) en la ISSAI 5300 Directrices sobre auditoría de TI, e incrementa técnicas de auditoría forense.

De la comparación de bases de datos de informes enviados por la Contraloría General del Estado a la Fiscalía y de los casos de delitos informáticos difundidos en el internet en entidades públicas, se determinó que existen delitos sancionados como peculado; sin embargo, estos se realizaron usando herramientas tecnológicas, por lo que se concluye lo siguiente:

- Las sanciones emitidas en el Código Integral Penal entre delitos informáticos tienen sanciones bajas en comparación a los delitos en contra de la administración pública.

- Todos los delitos en contra de la administración pública ejecutados con el uso de las TICs, se encuentran inmersos dentro de los delitos informáticos establecidos en el COIP.

En el nivel de conocimientos y experiencia en delitos informáticos se determinó que los auditores de TIC deben conocer y capacitarse en herramientas que permitan la detección de vulnerabilidades de sistemas de información y procesos de verificación en controles y monitoreo de las TIC implementas en la organización, en relación con normativa internacional y nacional vigente

Bibliografía:

Alcívar, C., Blanc, G., y Calderón, J. (2018). Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su punibilidad. Espacios, 1-10.

Arias M, M., y Domingos S, R. (2016). El desarrollo científico-tecnológico y su impacto en las auditorías y el control de la gestión empresarial. Revistas de La Universidad de Oriente, 58-71. Obtenido de https://revistas.uo.edu.cu/index.php/aeco/article/download/1340/1328

Cáceres, G., y De La Torre, C. M. (2017). Auditoría forense como medio para combatir la corrupción. Revista de Postgrado Arjé, 11(21), 88-97.

Código Orgánico Integral Penal. (2014). Registro Oficial Suplemento 180 de 10-feb.-2014. Ecuador.

Colás, A. (2016). EL DELITO DE INTRUSISMO INFORMÁTICO TRAS LA REFORMA DEL CP ESPAÑOL DE 2015. Revista Boliviana de Derecho (21), 210-228.

Constitución de la República del Ecuador. (20 de 10 de 2008). Registro Oficial 449.

Fiscalía General del Estado. (s.f.). Obtenido de https://www.fiscalia.gob.ec/los-delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje/

Gómez M, F. (2014). Competencia digital en la auditoría. Soporte o carga en el ejercicio profesional de los auditores. Cuadernos de Contabilidad, http://revistas.javeriana.edu.co/index.php/cuacont/article/view/9005.

Gonzáles, J., Bermeo, J., Villacreses, E., y Guerrero, J. (2018). Delitos informáticos: una revisión en Latinoamérica. Conference Proceedings, http://investigacion.utmachala.edu.ec/proceedings/index.php/utmach/article/view/262.

Instituto Nacional de Estadísticas y Censos. (2015). Metodología del Módulo de Tecnologías de la Información y Comunicación (TIC) en las Encuestas de Manufactura y Minería, Comercio Interno y Servicios 2015.

INTOSAI. (s.f.). Organización Internacional de las Entidades Fiscalizadoras Superiores. Obtenido de http://www.intosai.org/

ISSAI 5300. (2016). Directrices sobre auditoría de TI. Obtenido de Organización Internacional de las Entidades Fiscalizadoras Superiores: http://www.intosai.org/es/issai-executive-summaries/detail/detail/News/issai-5310-information-system-security-review-methodology-directriz-sobre-el-control-de-sistemas.html

Ley Orgánica de la Contraloría General del Estado. (18 de diciembre de 2015). Registro Oficial Suplemento 595 de 12-jun.-2002. Ecuador.

Loredo G, J. A., y Ramírez G, A. (2013). Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. Celerinet, 44-51.

Madariaga, J. (2004). Manual Práctico de Auditoría. Barcelona: T.G. Soler.

Montoya C, R. I. (2009). La Informatica Forense Como Ciencia Sistematica. Revista de Información, Tecnología y Sociedad, 3-8. Obtenido de

<http://www.revistasbolivianas.org.bo/scielo.php?script=sci_arttext&pid=S1997-40442009000200001&lng=es&nrm=iso>

Mora Q, E. (2017). Auditoría Informática. BOLETIN DEL IAICR (26), 12.

Normas de Control Interno. (16 de noviembre de 2009). Registro Oficial 78 de 1 de diciembre de 2009. Ecuador.

Normas Ecuatorianas de Auditoría Gubernamental. (2015). Acuerdo 019-CG en el Registro Oficial Registro Oficial Suplemento 6 de 10-oct.-2002. 21.

Ocampo S, C. A., Trejos B, O. I., y Solarte M, G. R. (2010). LAS TÉCNICAS FORENSES Y LA AUDITORIA. Scientia Et Technica, XVI (45), 108-113.

ODILA. (2017). Obtenido de https://www.odila.org/pdf/Informe_ODILA_2017.pdf

Página Web de la Contraloría General del Estado. (s.f.). Obtenido de Descargas: www.contraloria.gob.ec

Página Web del Consejo de la Judicatura. (s.f.). Obtenido de SISTEMA PERICIAL - Consulta de peritos acreditados: https://appsj.funcionjudicial.gob.ec/perito-web/pages/peritos_nacional.jsf

Palíz, O. (2017). Propuesta de complemento al artículo 410 de la Norma de Control Gubernamental Moderno emitida en el año 2009 por la Contraloría General del Estado del Ecuador sobre las tecnologías de la información y comunicaciones, aplicando estándares y buenas práctica. Propuesta de complemento al artículo 410 de la Norma de Control Gubernamental Moderno emitida en el año 2009 por la Contraloría General del Estado del Ecuador sobre las tecnologías de la información y comunicaciones, aplicando estándares y buenas práctica. Ecuador IAEN.

PLAN NACIONAL PARA EL BUEN VIVIR 2013 2017. (2015). Registro Oficial Suplemento 78 de 11-sep.-2013. Ecuador.

Pons, G. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad/ Internet, the new age of crime: cibercrime, ciberterrorism, legislation and cibersecurity. Revista Latinoamericana de Estudios de Seguridad, https://doi.org/10.17141/urvio.20.2017.2563.

Villamizar, C., Orjuela, A., y Adarme, M. (2015). Análisis Forense en Sistema de Información en el Marco Normativo Colombiano. Investigación E Innovación En Ingenierías, 3(1), 9-16.