DISEÑO E IMPLEMENTACIÓN DE UN PROCEDIMIENTO PARA LA RECOLECCIÓN, CADENA DE CUSTODIA Y USO DE EVIDENCIA DIGITAL DENTRO DEL DESARROLLO DE PRUEBAS DE AUDITORIA EN LA GERENCIA DEPARTAMENTAL VALLE DEL CAUCA DE LA CONTRALORIA GENERAL DE LA REPUBLICA

YEIMY ANDRES ARTEAGA GUERRON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTIAGO DE CALI
2018

DISEÑO E IMPLEMENTACIÓN DE UN PROCEDIMIENTO PARA LA RECOLECCIÓN, CADENA DE CUSTODIA Y USO DE EVIDENCIA DIGITAL DENTRO DEL DESARROLLO DE PRUEBAS DE AUDITORIA EN LA GERENCIA DEPARTAMENTAL VALLE DEL CAUCA DE LA CONTRALORIA GENERAL DE LA REPUBLICA

YEIMY ANDRES ARTEAGA GUERRON

Proyecto de Grado

Esp. Daniel Felipe Palomo Luna
Director de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTIAGO DE CALI
2018

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del Jurado

_____
Firma del Jurado

Cali, 27 de febrero de 2018

Cada logro alcanzado en la vida es un nuevo paso en el futuro y este nuevo logro en mi vida lo quiero dedicar principalmente a:

Mi hijo, esa pequeña extensión nuestra que con sus ojos, risas y sus muestras de amor, han sabido llenarme cada día de la motivación y fuerza para seguir adelante.

Mi esposa, quien con su amor, comprensión y paciencia ha sabido darme la fuerza y motivación para empezar, mantenerme y culminar cada nuevo proyecto de vida.

Mi madre, quien con su gran amor y esfuerzo, durante toda su vida, hizo todo lo posible para que hoy pueda encontrarme en el lugar donde estoy.

Mi familia que con sus palabras, detalles y aliento me ayudaron a mantener mis pasos siempre hacia adelante.

AGRADECIMIENTO

Durante esta nueva etapa, en la que alcanzo un nuevo logro, gracias a la exitosa culminación de este proyecto de grado y de vida, quiero expresar mis sinceros agradecimientos a:

- ✓ Dios, por la vida, por lo que tengo y por lo que soy.
- ✓ Mi Entidad, por darme la oportunidad de aplicar mis nuevos conocimientos en aras de brindar herramientas para mejorar nuestra labor encomendada.
- ✓ La Universidad Nacional Abierta y a Distancia – UNAD, por abrirme sus puertas para formarme profesionalmente como un especialista y permitirme ampliar mis conocimientos en el área de la Seguridad Informática.
- ✓ Mi director de proyecto, ingeniero Daniel Felipe Palomo Luna, quien con sus acertadas observaciones, recomendaciones, experiencia y conocimientos, fue mi guía para culminar exitosamente el presente trabajo y obtener mi título como especialista.
- ✓ A los tutores que, a través de la Universidad, impartieron sus conocimientos y me permitieron tener las bases para idear, planear y desarrollar este proyecto.
- ✓ A mi familia, motor que me impulsa a buscar nuevos horizontes, alcanzar nuevas metas y seguir siempre adelante.
- ✓ A amigos, compañeros y cada persona que con una frase, un gesto, una palabra de aliento, me animaron para seguir, a pesar de las circunstancias.

A todos muchas gracias.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ARCHIVO ELECTRÓNICO O DIGITAL: todo documento que contiene un conjunto de datos y que se genera, procesa o utiliza en un dispositivo electrónico como un computador, servidor u otros relacionados y que debe ser guardado en un medio de almacenamiento digital.

AUTENTICACIÓN: propiedad de la información que permite identificar quien la ha generado.

CADENA DE CUSTODIA: procedimiento que se aplica a la evidencia física o digital relacionada con una situación investigada, la cual incluye desde la recolección hasta el análisis realizado por los peritos, y que tiene como propósito evitar alteraciones, contaminaciones o destrucciones de dicha evidencia que puedan afectar los procesos que las incluyan como material probatorio.

CODIGO HASH: código alfanumérico que se obtiene mediante la aplicación de funciones y uso de algoritmos criptográficos ejecutados sobre un archivo. Permite establecer un código único para cada archivo con el fin de garantizar su integridad y controlar la realización de modificaciones a los mismos.

CONFIDENCIALIDAD: propiedad que impide que la información sea difundida o divulgada a usuarios o procesos que no se encuentren autorizados por las políticas de seguridad establecidas, asegurando que la misma solo estará disponible para usuarios o entidades autorizadas.

DBMS: sistema gestor de bases de datos por sus siglas en inglés (Data Base Management System). Es un conjunto de programas de software que se encargan de la creación y administración (almacenamiento, modificación y extracción de datos) de las bases de datos que se crean en estos entornos. Permiten además realizar consultas, generación de reportes y análisis de los datos almacenados.

DISPONIBILIDAD: esta propiedad establece que la información se encontrará disponible, en el momento que lo necesiten, para los usuarios que puedan acceder y hacer uso de ella.

IDEA: es un producto de software que permite la importación de archivos planos, bases de datos, hojas de cálculo, para realizar consultas y análisis de datos, estadísticas, y la generación de reportes, basados en criterios determinados por el especialista que lo usa.

INTEGRIDAD: característica que busca que los datos se mantengan libres de manipulación o alteraciones que modifiquen la información impidiendo asegurar que la misma se mantenga exacta, tal cual como fue generada.

IRREFUTABILIDAD: característica de la información por medio de la cual se asegura que los datos transmitidos fueron remitidos por el emisor especificado y/o que la información fue recibida por el receptor que se especifica en la transmisión.

MD5: algoritmo criptográfico computacional que permite realizar cálculos matemáticos de acuerdo con los datos contenidos en un archivo, para generar un valor que lo identifica como único.

MEDIO DE ALMACENAMIENTO DIGITAL: soportes físicos tales como CD, DVD, Pendrive USB, tarjetas SD y otros similares que permitan guardar archivos digitales o electrónicos para ser compartidos o transportados.

MICROSOFT EXCEL: hoja de cálculo de la empresa Microsoft que permite generar tablas de datos numéricos, alfanuméricos, organizados y sobre los cuales se puede ejecutar funciones y fórmulas para realizar cálculos matemáticos y operaciones de búsqueda o comparación entre diferentes fuentes.

NIVEL DESCONCENTRADO: esta forma de organización se crea con el propósito de brindar una mejor atención y eficacia ante el desarrollo de los asuntos de su competencia. En este grupo se encuentran entes, departamentos, gerencias, que no tienen personalidad jurídica ni patrimonio propio ya que se encuentran jerárquicamente subordinados y por tanto dependientes del nivel central de la organización o entidad a la que pertenecen. Tienen competencia para atender los asuntos y funciones que por ley han sido asignados dentro de su ámbito territorial.

PENDRIVE USB: dispositivo de hardware que permite el acopio y almacenamiento de información digital o electrónica como imágenes, música, documentos, entre otros. Su conexión se realiza por medio de puertos USB (Universal Serial Bus).

POSTGRESQL: es un DBMS de código abierto que permite importar, crear y exportar datos y bases de datos. También se permite la realización de consultas utilizando el lenguaje de consultas SQL.

SQL: (Structured Query Language), lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ellas, tales como consultas, comparaciones y otros.

SQL SERVER EXPRESS: es un DBMS con licencia gratuita de la empresa Microsoft. Permite realizar todas las funciones de un DBMS con la limitante en la cantidad y el tamaño máximo en bytes de las bases de datos que gestiona.

TOKEN: dispositivo de hardware similar a un pendrive USB que permite el almacenamiento de información o credenciales de seguridad como usuarios, claves,

seriales y otros para el uso de software o equipos de cómputo sin tener que digitar dicha información de autenticación.

USATI: dependencia de la Contraloría General de la República cuyas siglas significan Unidad de Seguridad y Aseguramiento Tecnológico e Informático. Tiene entre sus funciones prestar apoyo profesional y técnico para la formulación y ejecución de políticas y programas de seguridad de los servidores públicos, de los bienes y de la información de la entidad.

RESUMEN

Los resultados de pruebas de auditoría, obtenidos a través de la recolección y análisis de evidencia digital, deben contar con los requerimientos necesarios e idóneos para ser tenidos en cuenta como acervo probatorio dentro de un proceso de responsabilidad fiscal que pueda surgir del ejercicio auditor; sin embargo, los instrumentos actuales que posee la Gerencia Departamental del Valle del Cauca para realizar esta labor, no garantizan totalmente la eficiencia requerida en el desarrollo de labores que permitan asegurar que la evidencia digital cumpla con los requisitos para ser tenida en cuenta como prueba de lo observado. El no contar con un procedimiento claramente establecido no permite asegurar la integridad y confiabilidad de los datos y/o el medio físico que la almacena.

El presente trabajo buscó identificar los riesgos que actualmente se evidencian en la forma como se recauda la información digital para establecer así un procedimiento con unos pasos específicos para la recolección o recepción, almacenamiento y uso de la información digital que busca garantizar que las pruebas obtenidas, basadas en evidencia digital, tengan la fuerza probatoria suficiente para ser tenidas en cuenta como soporte idóneo dentro de un proceso que busca resarcir un daño fiscal.

INTRODUCCIÓN

Los avances tecnológicos han permitido, día a día, que los diferentes procesos y actividades llevadas a cabo en las diferentes empresas, estamentos, instituciones y aún en los hogares se realicen de una manera automatizada, reduciendo la ocurrencia de fallas o inconsistencias asociadas al error humano.

La informática, especialmente, ha permitido que hoy en día los diferentes procesos se realicen con la ayuda de herramientas de hardware y software que pueden realizar cálculos y ejecutar instrucciones, en un periodo de tiempo reducido, comparado con las actividades manuales, e incrementando confiabilidad a los resultados generados.

La implementación de este tipo de herramientas en las entidades, exige a las firmas auditoras que obtengan evidencia en formatos digitales tales como hojas de cálculo en Excel, reportes planos generados por los sistemas de información y/o aplicativos institucionales, mensajes de correo electrónico entre otros; por esto, se requiere establecer técnicas precisas para la obtención, manejo y uso de evidencia en formatos digitales para garantizar su confidencialidad, integridad y disponibilidad en el análisis de los procesos y procedimientos realizados por la institución o entidad auditada.

En Colombia se ha creado la Contraloría General de la República como el órgano máximo de control fiscal del país, quien es el encargado de velar por el uso adecuado, y ceñido a los ordenamientos normativos, de los recursos públicos del orden nacional por parte de las Entidades Oficiales y particulares que reciben estos recursos por parte del Estado para cumplir funciones establecidas por la legislación colombiana.

La Contraloría General de la República no es ajena al avance tecnológico del país y las entidades vigiladas, razón por la cual se hace necesaria la existencia de procedimientos técnicos, precisos y confiables que permitan ejecutar la labor de control fiscal con un alto grado de eficiencia, efectividad y confiabilidad en aras de tener un panorama claro del comportamiento de las instituciones auditadas y el uso que estos hacen de los recursos entregados por el Estado para el cumplimiento de sus labores establecidas por la Ley.

El presente proyecto pretende, mediante el análisis y estudio de actividades, información, técnicas y medios de almacenamiento, la creación e implementación de un procedimiento que permita a la Contraloría General de la República realizar pruebas de auditoría, de manera más eficiente y eficaz, a los soportes de información almacenados en medios digitales de los proyectos, contratos y labores realizados por los entes vigilados.

1. TITULO

Diseño e implementación de un procedimiento para la recolección, cadena de custodia y uso de evidencia digital dentro del desarrollo de pruebas de auditoria en la Gerencia Departamental Valle Del Cauca de la Contraloría General de la Republica.

2. FORMULACIÓN DEL PROBLEMA

Los resultados de pruebas de auditoría, obtenidos a partir de la recolección y análisis de evidencia digital (archivos digitales, bases de datos), deben contar con los requerimientos necesarios e idóneos para ser tenidos en cuenta como acervo probatorio dentro de un proceso de Responsabilidad Fiscal que pueda surgir del ejercicio auditor; sin embargo, actualmente los medios, mecanismos, procedimientos e instrumentos con los que la Gerencia Departamental del Valle del Cauca cuenta para realizar esta labor, no garantizan totalmente la eficiencia requerida en el desarrollo de labores de obtención de evidencia digital que permita asegurar que dicha evidencia cumpla con los requisitos para ser tenida en cuenta como ilustración suficiente de la situación observada.

Al no contar con herramientas o procedimientos claramente definidos para el manejo de este tipo de evidencia, no se puede asegurar su integridad y confiabilidad tanto a nivel de los datos que la componen como el medio físico que la almacena.

Un proceso de Responsabilidad Fiscal que se base en una prueba ejecutada sobre información almacenada en medios digitales puede no tener la certeza suficiente o la garantía de que esa información corresponde a la realidad del ente auditado y que la misma, de acuerdo con la normatividad relacionada, fue tomada garantizando que corresponde a información oficial de la entidad. Una prueba que no cumple con estos requisitos ocasiona que un proceso se declare nulo al no cumplir el debido proceso o no garantizar que corresponde a una fuente oficial y se haya obtenido correctamente de la fuente.

2.1. PLANTEAMIENTO DEL PROBLEMA

¿Cómo el diseño e implementación de un procedimiento para la recolección, cadena de custodia y uso de evidencia digital dentro del desarrollo de pruebas de auditoría garantiza la idoneidad y validez de dicha evidencia, obtenida dentro de una auditoría gubernamental en la Gerencia Departamental Valle Del Cauca de la Contraloría General de la Republica?

3. JUSTIFICACION

La evidencia digital ha ganado importancia en el ámbito del control fiscal ejercido sobre las entidades del Estado, siendo imperante lograr que las mismas permitan tener certeza de la gestión y manejo de los recursos públicos. La falta de un procedimiento claro que garantice la confiabilidad, pertinencia y suficiencia de las pruebas obtenidas a partir de medios digitales, genera el riesgo de que las mismas no sean tenidas en cuenta y no se tenga certeza de lo evidenciado durante el ejercicio del proceso auditor en la Gerencia Departamental Colegiada Valle del Cauca de la Contraloría General de la República.

Teniendo en cuenta el uso masivo de recursos informáticos y la importancia que la información tiene, se hace necesario establecer mecanismos y procedimientos estándares para la recolección, identificación, uso y análisis de la información en medios digitales, que garanticen que los resultados obtenidos como prueba dentro de un informe de auditoría o un proceso de responsabilidad fiscal cumplan los requerimientos normativos y las condiciones que la ley establece para ser considerados como válidos.

Muchas veces, los resultados de las auditorías se sustentan en evidencia, información y datos digitales obtenidos durante la realización de las pruebas, por lo cual es un gran beneficio contar con un adecuado procedimiento que garantice que la evidencia electrónica sea obtenida, analizada y conservada adecuadamente, manteniendo su idoneidad, confiabilidad, integridad y suficiencia ante la situación detectada. Por esto, es necesario contar con un procedimiento estandarizado que permita asegurar un alto grado de certeza y confiabilidad en los datos obtenidos como evidencia dentro de las actividades del Ente de Control Fiscal para, de este modo, cumplir con la labor de vigilar el uso adecuado de los recursos públicos de la nación y garantizar el cumplimiento de la normatividad, orientados a satisfacer las necesidades del pueblo colombiano.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Implementar un procedimiento de recolección, cadena de custodia y uso de evidencia digital que permita garantizar la idoneidad y validez de dicha evidencia, obtenida dentro de una auditoría gubernamental como prueba suficiente, confiable y pertinente en la Gerencia Departamental Valle Del Cauca de la Contraloría General de la Republica.

4.2. OBJETIVOS ESPECÍFICOS

- Definir los tipos de información y medios idóneos que se deben utilizar para la recolección de evidencia digital.

- Establecer los pasos, medios y responsables para el manejo y control de la evidencia digital recaudada en las auditorías.

- Formalizar las herramientas de software idóneas para el análisis y uso de la evidencia digital, orientadas a obtener resultados claros, confiables y que revelen la realidad de lo observado.

- Verificar, mediante una prueba piloto, la efectividad y eficiencia de los procedimientos, herramientas y pasos establecidos para garantizar la validez e idoneidad de la evidencia digital recaudada.

- Diseñar un procedimiento para la recolección, cadena de custodia y uso de la evidencia digital obtenida a partir de la práctica de pruebas de auditoría.

5. MARCO DE REFERENCIA

5.1. ANTECEDENTES

Como se ha ilustrado, la evidencia digital es un elemento que ha ganado importancia en las labores que las entidades de vigilancia y control del Estado realizan, para garantizar el cumplimiento de las normas y el adecuado uso de los recursos públicos.

La incursión en el uso de información en medios digitales y por lo tanto de herramientas para su identificación, uso y disposición, ha obligado a la creación de procedimientos y herramientas para su adecuado manejo, adicional a los parámetros establecidos en la normatividad colombiana.

A continuación, se establecen los diferentes trabajos e investigaciones relacionadas con el desarrollo del presente trabajo:

- Tesis de Grado Manejo de evidencia digital en dispositivos de almacenamiento pendrive USB aplicando la norma ISO/IEC 27037:2012, presentada por el ingeniero José Bernardo Cortés de la Rosa, Especialización en Seguridad Informática de la Universidad Nacional Abierta y a Distancia UNAD. Año 2014.

Esta tesis, brinda información relacionada con el manejo de evidencia digital almacenada en dispositivos de almacenamiento USB en Colombia, acorde con la normatividad vigente en el país.

- Tesis de Grado Metodología para el desarrollo de procedimientos periciales en el ámbito de informática forense, presentado por Juan Miguel Tocados Cano, Tecnologías y Sistemas de Información de la Universidad de Castilla – La Mancha. Año 2015.

Trata sobre la preservación de la evidencia digital a través del uso de cadena de custodia y sus respectivos procedimientos y herramientas para su uso como prueba idónea en un proceso de índole penal.

- Tesis de Grado Cadena de custodia digital de las evidencias para la realización de un peritaje, presentada por Carlos Romeo García, facultad de Ingeniería de la Universidad de San Carlos de Guatemala. Año 2014.

Presenta en su trabajo, conceptualización de la cadena de custodia como elemento importante para garantizar la confiabilidad y autenticidad de una prueba de evidencia digital que deba ser usada en un proceso judicial. Adicionalmente,

presenta un marco base de cadena de custodia aplicable a la salvaguarda de evidencia digital.

- Tesis de Grado Análisis Jurídico y material de la evidencia digital en los delitos informáticos judicializados por la Fiscalía General de la Nación en el Municipio de Bucaramanga en el periodo 2006 – 2010, presentada por Paula Andrea Alvarez David, Escuela de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana en Bucaramanga, Santander. Año 2011.

Ilustra las implicaciones legales de una adecuada práctica de pruebas que involucra evidencia digital.

- Manual Básico de Cateo y Aseguramiento de Evidencia Digital, Elaborado por Gabriel Andrés Campoli.

Sirve como guía de las acciones y mecanismos mínimos a aplicar para el cateo o aseguramiento de los equipos electrónicos y evidencia digital encontrados en la escena de un crimen.

- El manejo de la prueba electrónica en el proceso civil colombiano, publicado por Nattan Nisimblat de la Facultad de Derecho de la Universidad de los Andes. Año 2010.

Estudio realizado sobre el manejo de la prueba electrónica desde su producción, pasando por su recolección, hasta su análisis.

- Artículo Evidencia digital y técnicas y herramientas de auditoría asistidas por computador, elaborado por Francisco Javier Valencia Duque y Johnny Alexander Tamayo Arias, Facultad de Ciencias e Ingeniería, Universidad de Manizales.

- Articulo Cadena de Custodia en el Análisis Forense. Implementación de un Marco de Gestión de la Evidencia Digital, elaborado por Tomás Marqués-Arpa y Jordi Serra-Ruiz, Estudios de Informática, Multimedia y Telecomunicación. Universitat Oberta de Catalunya.

Presenta una propuesta para la implementación de una cadena de custodia digital y segura. Se contempla una serie de pasos consecutivos vistos como eslabones, con sus respectivas marcas y registros digitales que buscan que la prueba no pierda el valor jurídico requerido.

5.2. MARCO CONTEXTUAL

La Contraloría General de la República (CGR) es el máximo órgano de control fiscal del Estado. Como tal, tiene la misión de procurar el buen uso de los recursos y bienes públicos y contribuir a la modernización del Estado, mediante acciones de mejoramiento continuo en las distintas entidades públicas[1].

Como lo menciona la CGR[2], para dar cumplimiento a lo ordenado en la Constitución Nacional, evalúa los resultados obtenidos por las organizaciones y entidades del Estado vigiladas al determinar si adquieren, manejan y/o usan los recursos públicos conforme a la normatividad establecida y acatando los principios de economía, eficiencia, eficacia, equidad y sostenibilidad ambiental.

Adicionalmente la CGR[3], resultado del ejercicio auditor (Vigilancia Fiscal), establece la responsabilidad fiscal de los servidores públicos y de los particulares que causen, por acción o por omisión y en forma dolosa o culposa, un daño al patrimonio del Estado, tras lo cual puede dar lugar a la imposición de sanciones pecuniarias que correspondan y las demás acciones derivadas del ejercicio de la vigilancia fiscal.

Para ejercer la función como Órgano de Control Fiscal en el país, la Contraloría General de la República se encuentra organizada como una Entidad del nivel desconcentrado, conformado por un Nivel Central y 32 Gerencias Departamentales Colegiadas, encargadas de realizar Vigilancia Fiscal en cada uno de los departamentos.

Las Gerencias Departamentales Colegiadas se componen de 3 grupos específicos encargados de realizar control fiscal en diferentes campos y/o etapas del proceso establecido en la Ley 80 de 1993:

Vigilancia Fiscal: encargado de la realización de auditorías a las Entidades vigiladas, orientadas a examinar que la administración y uso de recursos públicos de la Nación a su cargo, se ajusten a lo establecido por la Ley.

Participación Ciudadana: Atención de las denuncias de origen ciudadano sobre el incorrecto uso de los recursos públicos de la Nación, las cuales son atendidas por funcionarios auditores para emitir una respuesta al ciudadano.

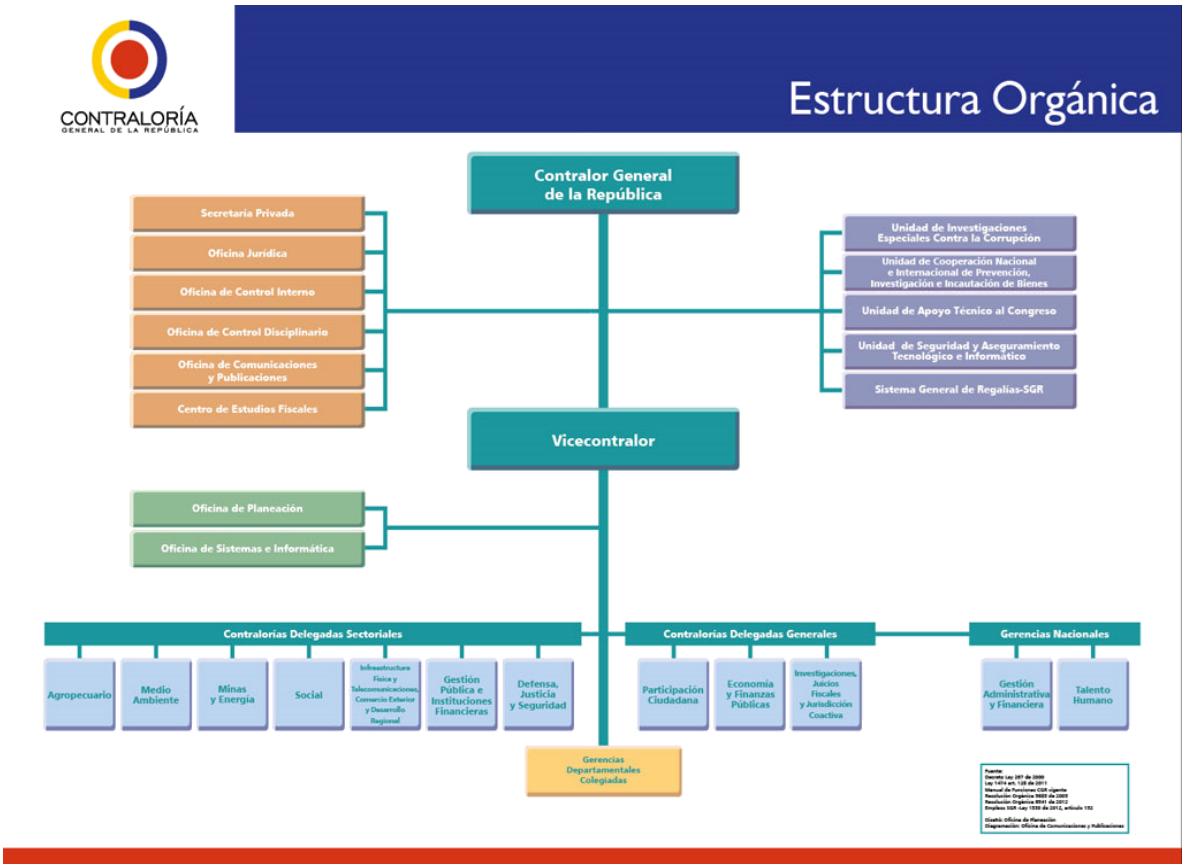
---

[1] CONTRALORÍA GENERAL DE LA REPÚBLICA. Qué es la Contraloría? [en línea]. <http://www.contraloria.gov.co/web/guest/que-es-la-cgr> [citado en 27 de septiembre de 2015]

[2] CONTRALORÍA GENERAL DE LA REPÚBLICA. Qué hace la CGR? [en línea]. <http://www.contraloria.gov.co/web/guest/que-es-la-cgr> [citado en 27 de septiembre de 2015]

[3] CONTRALORÍA GENERAL DE LA REPÚBLICA. Qué hace la CGR? [en línea]. <http://www.contraloria.gov.co/web/guest/que-es-la-cgr> [citado en 27 de septiembre de 2015]

Figura 1. Organigrama Contraloría General de la República



Fuente: http://www.contraloria.gov.co/contraloria/la-entidad/organigrama-y-dependencias

Responsabilidad Fiscal: Los hallazgos con incidencia fiscal, obtenidos como resultado de auditorías o atención de denuncias, se trasladan a este grupo para adelantar un proceso que permita determinar con precisión el daño causado, los responsables de dicho daño, en búsqueda de lograr su resarcimiento.

5.3. MARCO TEORICO

5.3.1. Informática Forense. De acuerdo con el Doctor Jeimy J, Cano[4], existen varias definiciones de informática forense entre las cuales es importante resaltar que es la *"Disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso"*; o *"Como la disciplina científica y especializada que*

[4] CANO, J. Introducción a la informática forense. En: Sistemas. no. 96, p. 64-73.

entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos".

Según Cano, estas dos definiciones son complementarias, toda vez que una de ellas se centra en las consideraciones forenses y la otra se ubica en la especialidad técnica, buscando con ello determinar la existencia u ocurrencia de hechos a partir del análisis de evidencia digital que sirva como soporte válido y suficiente dentro de un proceso judicial.

Además, el Doctor Cano ilustra que esta disciplina es una forma de ayudar en los procesos judiciales, mediante la búsqueda de criminales o la explicación de sucesos, eventos o hechos, por la aplicación de procedimientos de la criminalística a los medios y elementos informáticos, los cuales son de amplio uso en la actualidad.

De acuerdo con Ghosh[5], la informática forense también se puede definir como *"una disciplina emergente dedicada a la recolección de evidencia digital o computacional para ser utilizada con propósitos judiciales"*.

Con base en lo anterior, se puede decir entonces que la informática forense es un conjunto de prácticas orientadas a determinar los sucesos de un caso determinado, a partir de la correcta recolección, custodia y análisis de los datos e información almacenada en medios informáticos, preservando su integridad y garantizando su procedencia y pertinencia dentro de la situación investigada.

5.3.1.1. *Definición de Evidencia Digital.* Según Ghosh[6], la Evidencia Digital se define como la información que, mediante actividad humana u otro tipo de técnica semejante, se ha obtenido o ha sido extraída de un medio o dispositivo informático.

De acuerdo con esto, evidencia digital es toda información o registro almacenado en un computador o dispositivo informático que puede ser extraído y ser utilizado como prueba o evidencia soporte en un proceso legal y/o judicial.

Para el caso específico del presente estudio, se puede decir que este tipo de evidencia puede ser parte del material probatorio necesario y utilizado dentro del desarrollo de un proceso de responsabilidad fiscal en el cual se busca establecer la existencia de un presunto daño patrimonial.

5.3.1.2. *Cadena de Custodia.* La cadena de custodia, en lo relacionado con el manejo y preservación de evidencia digital, se refiere a un procedimiento

---

[5] CALAMEO.COM. Guía Para El Manejo De Evidencia Digital [en línea]. <http://es.calameo.com/read/004053479c7bcc08c68de>. [citado el 26 de octubre de 2015]

[6] CALAMEO.COM. Guía Para El Manejo De Evidencia Digital [en línea]. <http://es.calameo.com/read/004053479c7bcc08c68de>. [citado el 26 de octubre de 2015]

establecido desde el momento de su recolección en el lugar de los hechos, hasta su valoración por parte de los encargados de administrar justicia.

Con este procedimiento se busca que la evidencia digital recaudada, y por tanto la información que ésta contiene, mantenga sus características originales, evitando alteraciones, sustituciones o cualquier tipo de contaminación durante el proceso judicial o fiscal en el cual se encuentra incluida como parte del acervo probatorio.

Para garantizar su adecuada conservación, se debe llevar un registro riguroso y detallado del material probatorio para así identificar de manera individual la evidencia recaudada mediante datos de identificación únicos tales como poseedores, lugar, hora, fecha, nombres, dependencia involucrada entre otros.

También debe tenerse en cuenta que este tipo de información o datos se encuentran almacenados o registrados en dispositivos magnéticos o digitales que requieren de un correcto almacenamiento y organización con el fin de contar con todas las características que garanticen la inocuidad y la esterilidad técnica en el manejo de los mismos durante las diferentes etapas y procesos que requieran de su consulta.

El cumplimiento estricto de los pasos y procedimientos establecidos en la cadena de custodia permite garantizar la idoneidad de la prueba dentro de un proceso judicial, penal o fiscal.

5.3.1.3. *Consideraciones Jurídicas.* Cano[7], sobre este tema expone que la evidencia digital, independiente del medio en el que se encuentre, debe avanzar hacia una estrategia de formalización, que brinde un elemento formal para su evaluación y análisis dentro del ordenamiento judicial de un determinado país.

Dentro de las legislaciones de muchos países, se ha establecido que, para ser admitida o tenida en cuenta como prueba dentro de un proceso, la evidencia digital debe cumplir con los siguientes aspectos:

- Autenticidad
- Confiabilidad
- Suficiencia
- Conformidad con las leyes.

La autenticidad de la evidencia se refiere a que esta se haya generado y referenciado en los lugares relacionados con el caso o proceso examinado. Se refiere también a que la misma no haya sufrido alteraciones y que por tanto corresponde a la realidad de la situación examinada.

[7] CANO MARTÍNEZ, Jeimy J. Computación forense. Descubriendo los rasgos informáticos. México, D.F.: Alfaomega, 2009. 344 p. ISBN 978-958-682-767-6.

Por otro lado, la confiabilidad de una prueba se relaciona con el hecho de que la evidencia recolectada y aportada a un proceso proviene de una fuente creíble y verificable.

En cuanto a la suficiencia, se busca que se presente la cantidad necesaria de material probatorio que permita asegurar que la situación presentada como delito o que represente una falta a la normatividad vigente, pueda ser soportada en las pruebas de manera completa y clara.

Por último, la conformidad con las leyes establece que los mecanismos y métodos utilizados para la recolección, preservación y análisis de la evidencia digital, se ajuste a la normatividad del país o lugar donde se presenta. No obstante existir lineamientos y estándares internacionales, se debe tener en cuenta que su aplicación se ajuste a la legislación o normatividad relacionada para el caso y lugar de los hechos.

Es importante que toda evidencia digital cumpla con estos cuatro conceptos con el fin de garantizar que una prueba basada en evidencia digital soporte total y adecuadamente un hallazgo o situación evidenciada en un proceso jurídico o de responsabilidad fiscal para el caso del presente proyecto.

5.3.2. Norma ISO / IEC 27037:2012. Esta norma internacional provee orientaciones sobre mejores prácticas en la identificación, adquisición y preservación de evidencias digitales potenciales que permitan aprovechar su valor probatorio. Se orienta su uso a las investigaciones en las cuales interviene el uso de recursos electrónicos o digitales.

Define dos roles de especialistas en el manejo y administración de las evidencias electrónicas:

- Digital Evidence First Responders (DEFR). Experto en primera intervención de evidencias electrónicas
- Digital Evidence Specialists (DES). Experto en gestión de evidencias electrónicas

La norma ISO / IEC 27037:2012 se enfoca en el tratamiento de los siguientes dispositivos:

- Medios de almacenamiento digitales utilizados en ordenadores tales como discos duros, discos flexibles, discos ópticos y magneto ópticos, dispositivos de datos con funciones similares
- Teléfonos móviles, asistentes digitales personales (PDA), dispositivos electrónicos personales (PED), tarjetas de memoria

- Sistemas de navegación móvil
- Cámaras digitales y de video (incluyendo CCTV)
- Ordenadores de uso generalizado conectados a redes
- Redes basadas en protocolos TCP / IP y otros.
- Dispositivos con funciones similares a las anteriores

Estas son las características de la norma que se ajustan al proyecto:

- Está orientada al manejo de la evidencia digital, buscando garantizar que dicha evidencia se ajusta a los requerimientos judiciales.
- Es una norma de amplia aplicación, ya que cubre una gran variedad de dispositivos y situaciones a examinar.

5.3.2.1. *Orientaciones de la norma sobre Evidencia Digital.* La norma establece los principios de relevancia, confiabilidad y suficiencia de la evidencia obtenida a partir de dispositivos informáticos. Los principios mencionados se definen así:

- Relevancia: La evidencia digital obtenida debe estar relacionada con los hechos investigados.
- Confiabilidad: La certeza que la evidencia digital obtenida no ha sido alterada en ningún caso, desde su identificación, recolección, preservación y análisis hasta su presentación en el proceso en que es requerida.
- Suficiencia: La evidencia por sí misma debe ser suficiente para explicar el hecho evidenciado y el cual es motivo de análisis.

Para el manejo de la evidencia digital, se definen tres etapas, las cuales corresponden a:

- Recolección.
- Adquisición.
- Preservación.

Todas las acciones que se realizan, relacionadas con el recaudo, manejo y cuidado o preservación de la evidencia digital obtenida, deben estar documentadas en sus diferentes etapas, y las mismas deben basarse por los siguientes principios:

- Minimizar el manejo de la evidencia digital
- Documentar cualquier acción que implique un cambio irreversible
- Adherirse a las regulaciones y leyes locales
- No extralimitarse en sus funciones

5.3.2.2. *Sobre la Cadena de Custodia.* La norma introduce el concepto de Cadena de Custodia (CoC por sus siglas en inglés). Establece como elementos mínimos que esta debe contener, los siguientes:

- Un identificador univoco de la evidencia.
- Quién accede a la evidencia, en qué momento y en qué ubicación física.
- El pasaje de la evidencia de un sitio a otro y tareas realizadas.
- Cualquier cambio inevitable potencial en evidencia digital será registrado con el nombre del responsable y la justificación de sus acciones.

5.4. MARCO CONCEPTUAL

5.4.1. Evidencia Digital en auditorias gubernamentales. En la actualidad, la información generada y procesada por las entidades que son sujeto de auditoría por parte de la Contraloría General de la República, se encuentra contenida en bases de datos que son administradas por sistemas de información o aplicaciones de computadora que permiten realizar diferentes tareas u operaciones sobre ellos de forma automática, ahorrando tiempos de procesamiento manual como en épocas anteriores.

El trabajo auditor se basa en las pruebas y verificaciones que se efectúen sobre toda la información que posee la entidad vigilada que evidencia todas sus actuaciones durante una vigencia determinada.

Producto de las pruebas realizadas por los auditores, se obtiene información que soporta las situaciones evidenciadas como acciones que no debieron realizarse o que no se ajustan a los lineamientos y directrices determinados por las leyes nacionales.

La información obtenida de medios digitales o electrónicos, y que sirve como soporte para evidenciar una situación o hallazgo de auditoría, se conoce como evidencia digital que es toda información o datos que se encuentran almacenados en dispositivos digitales o electrónicos, y que contienen el registro de los procesos y procedimientos efectuados por las entidades dueñas de esta información.

La evidencia digital recaudada dentro del desarrollo de un proceso auditor, al ser un tipo de información basada en medios electrónicos y no en formatos físicos como el papel, requiere de un procedimiento adicional que permita evidenciar, con posterioridad, que esta fue obtenida directamente de la fuente de manera oficial y formal, garantizando que la forma de adquisición o entrega se haya sujeto a los lineamientos establecidos para contar con la evidencia como soporte probatorio dentro de un informe de auditoría o una posterior indagación preliminar o proceso de responsabilidad fiscal de ser el caso.

5.4.2. Variables relacionadas con la Evidencia Digital. Para la norma ISO/IEC 27037:2012, la evidencia digital debe obedecer a tres principios fundamentales: relevancia, confiabilidad y suficiencia.

Estos tres principios permiten brindarle formalidad a las pruebas obtenidas basadas en evidencia digital, lo cual busca garantizar que dicha evidencia preste el mérito jurídico suficiente para soportar un hecho o situación direccionada a corroborar la responsabilidad de un sujeto dentro de una acción contraria a la ley.

5.4.2.1. *Relevancia.* Es una condición técnicamente jurídica, que trata de la pertinencia de elementos en una situación específica analizada para probar una hipótesis sobre los hechos investigados. Toda prueba o elementos probatorios que no cumplan con este requisito no serán tenidos en cuenta dentro del caso objeto de estudio.

5.4.2.2. *Confiabilidad.* Se refiere a la auditabilidad y repetibilidad de la evidencia recaudada. Quiere decir esto que, si unos resultados se obtuvieron en una prueba, otro auditor que analice los mismos hechos y ejecute las mismas pruebas debe obtener los mismos resultados.

5.4.2.3. *Suficiencia.* Indica que la evidencia digital obtenida es suficiente para sustentar los hallazgos y verificar las afirmaciones emitidas sobre la situación examinada y evidenciada. Este elemento está sujeto a la experiencia y formalidad del perito informático en el desarrollo de sus procedimientos.

Estas características ayudan a conformar un material probatorio basado en evidencia digital que preste el mérito como acervo probatorio dentro de un proceso jurídico o de responsabilidad fiscal.

Además, la normatividad colombiana requiere que las pruebas recaudadas cuenten con el peso suficiente para que no sean controvertidas.

5.4.3. Seguridad Informática y de la Información. Hoy en día, la facilidad de interconexión entre distintas entidades, personas y dispositivos, ha hecho que la información digital deba ser asegurada para garantizar que los datos no sean alterados y correspondan a la realidad del actuar del propietario de los mismos.

5.4.3.1. *Seguridad Informática.* Se relaciona con todas las medidas y controles que se establecen para garantizar que la información y los equipos que forman parte de una entidad, minimicen los riesgos de robo, pérdida o alteración de los datos que son el activo principal de una entidad en los tiempos actuales.

Las medidas de seguridad que se establezcan deben obedecer a un estudio previo en el cual se haya determinado de manera profesional y técnica, cuales son aquellas

situaciones que puedan permitir que la información se ponga en riesgo ante eventos internos o externos para los cuales no se haya previsto un control con anterioridad.

La seguridad informática es una rama importante hoy en día ya que busca garantizar que el componente informático de una empresa o entidad gubernamental cuenta con los mecanismos necesarios que permitan tener información confiable para la misma o, como en el caso del presente trabajo, de entidades de control gubernamental que basan sus pruebas y análisis en la información digital o electrónica recibida.

5.4.3.2. *Seguridad de la Información.* Corresponde a todas las medidas que se deben tomar para asegurar la información y los datos de una empresa o entidad.

A diferencia de la seguridad informática, la seguridad de la información busca asegurar toda la información existente, independientemente del medio (físico, digital u otros) en el que se encuentre almacenada.

La seguridad Informática busca mantener características importantes de la información para aseverar que la misma es confiable. Las características que debe cumplir la información son:

- Confidencialidad: Característica de la información que impide que los datos sean divulgados a personas, entidades y/o procesos no autorizados para su uso.
- Disponibilidad: Esta propiedad garantiza que la información se encuentra a disposición de los usuarios autorizados que la requieran en el momento que la necesiten.
- Integridad: Esta característica dice que la información debe mantenerse libre de modificaciones no autorizadas y ser exacta sin alteraciones o manipulaciones de personas no autorizadas.

Existen además servicios de seguridad que buscan confirmar la autenticidad y origen de los datos que se examinan:

- Autenticación: Esta propiedad es la que permite que se identifique con exactitud quien fue el emisor o productor de la información y no de un tercero intentando realizar suplantación.
- No repudio: Por medio de este servicio se confirma que un mensaje fue remitido por el emisor que se especifica en el mismo y/o que fue recibido por un usuario específico.

Para el caso objeto del presente trabajo, se busca que la información digital recibida durante el desarrollo de un proceso auditor, sea certificada por la Entidad con el fin de garantizar que:

- La información recibida por el equipo auditor, en respuesta a una solicitud formal, corresponda con la información oficial que la entidad produce.
- La información recaudada dentro de proceso de auditoría, se encuentre disponible para los análisis correspondientes en las diferentes etapas y procesos de la Contraloría General de la República.
- Se pueda saber, en cualquier etapa, que la información fue recaudada y recibida de acuerdo con los procedimientos legales que certifiquen que la misma se obtuvo adecuadamente.
- Los datos evaluados por el equipo auditor corresponden a los mismos datos que fueron suministrador por la entidad vigilada.

En todo caso, apoyados en la seguridad informática y específicamente en el uso de una cadena de custodia, el procedimiento desarrollado como producto resultado del presente trabajo, pretender servir de herramienta para garantizar que la información suministrada por la entidad cuente con todos los atributos necesarios para ser recibida, almacenada y procesada por la Contraloría General de la República, en aras de efectuar un examen ajustado a la realidad que genere resultados bien soportados que permitan dictaminar si la empresa o entidad evaluada ha ejecutado los recursos asignados conforma a la normatividad vigente y las directrices establecidas por las leyes nacionales.

5.5. MARCO LEGAL

La Contraloría General de la República, por mandato constitucional, tiene a cargo la función pública de ejercer control fiscal sobre los particulares o entidades del estado que administran o manejan fondos o bienes de la Nación. Esta función como máximo órgano de control fiscal se encuentra establecida en el artículo 267 de la Constitución Política de Colombia.

De acuerdo con lo establecido en el artículo 267, "*…Dicho control se ejercerá en forma posterior y selectiva conforme a los procedimientos, sistemas y principios que establezca la ley…*". Lo anterior implica que la Contraloría General de la República ejercerá su control de manera posterior a la ocurrencia de los hechos, razón por la cual las auditorías se programan para realizar verificación y seguimiento a las vigencias terminadas.

El Estado Colombiano, a través del Código de Procedimiento Civil, Sección tercera, Título XIII (Sin perjuicio de las disposiciones penales al respecto), establece el régimen probatorio. Entre otras cosas, el Código determina que las decisiones judiciales, deben estar fundadas en pruebas que sean oportunamente allegadas a un proceso, deben estar ceñidas al asunto materia y que también deberán rechazarse por el juez las que sean legalmente prohibidas o ineficaces, impertinentes y/o superfluas.

Otras normas de necesario estudio dentro del desarrollo del proyecto son:

Ley 527 de 1999, expedida por el Congreso de la República de Colombia. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 610 del 15 de agosto de 2000, expedida por el Congreso de la República de Colombia. Por la cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías.

Ley 1273 del 5 de enero de 2009, expedida por el Congreso de la República de Colombia. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Sentencia C-662 de 8 de junio de 2000, proferida por la Corte Constitucional de Colombia. Mediante esta sentencia se declaran exequibles los artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45 de la ley 527 de 1999.

Resolución 0-6394 del 22 de diciembre de 2004, emanada por la Fiscalía General de la Nación. Por medio de la cual se adopta el manual de procedimientos del Sistema de Cadena de Custodia para el Sistema Penal Acusatorio.

Acuerdo PSAA06-3334 del 2 de marzo de 2006, expedido por la Sala Administrativa del Consejo Superior de la Judicatura. Por el cual se reglamentan la utilización de medios electrónicos e informáticos en el cumplimiento de las funciones de administración de justicia.

6. DISEÑO METODOLÓGICO

6.1. METODOLOGÍA DE INVESTIGACIÓN

El enfoque que se utilizará para el desarrollo de este proyecto es cuantitativo. Se usará este enfoque por cuanto se medirá la eficiencia, integridad, pertinencia y confiabilidad de la evidencia digital que se recolecta en los procesos auditores, así como su idoneidad y validez en procesos en los que se busca demostrar un hecho real basado en estas pruebas.

La propuesta de investigación es de tipo exploratoria porque se busca explorar y analizar más a fondo las técnicas necesarias para la recolección y análisis de evidencia digital, pertinente y adecuada a las pruebas y soportes requeridos, que permita tener un conocimiento claro con el fin de generar un procedimiento acorde con las necesidades de la Entidad.

Es de tipo descriptiva porque se trata de describir los procedimientos y políticas que regulen el adecuado y correcto uso de la evidencia digital, así como su custodia parea garantizar su conservación y uso adecuado correspondiente con la normatividad legal colombiana.

Por último, se dice que es explicativa ya que se trata de explicar, a través del resultado final, los procedimientos y características de la evidencia digital a recolectar y usar para obtener un material probatorio válido, pertinente e idóneo.

6.1.1. Población y Muestra. La población universo son todos los funcionarios del área de Vigilancia Fiscal de la gerencia Departamental Colegiada del Valle del Cauca, quienes se encargan de realizar auditorías y obtener material probatorio que sustente las situaciones evidenciadas.

La muestra será tomada de un grupo auditor que haya realizado una auditoría gubernamental en la cual se involucre el uso de evidencia digital como material que soporta los hallazgos evidenciados.

6.1.2. Instrumentos de recolección de información. Como instrumentos para realizar la recolección de información para el desarrollo de este proyecto se utilizarán entrevistas, cuestionarios, papeles de trabajo y listas de chequeo.

6.2. METODOLOGÍA DE DESARROLLO

Durante el desarrollo del presente proyecto se llevará a cabo una serie de actividades orientadas a la obtención de información, análisis de datos y generación de una propuesta para la implementación de un procedimiento encaminado a la recolección, custodia y uso de la información suministrada, en medios digitales o electrónicos, por parte de las entidades sujeto del control ejercido por la Contraloría General de la República.

Con el fin de contar con el insumo suficiente para diseñar un procedimiento que se ajuste a las necesidades específicas de los funcionarios del grupo de vigilancia fiscal de la Contraloría General de la República, se efectuarán las siguientes actividades, acorde con los objetivos del proyecto, las cuales se realizarán en el orden que a continuación se establece.

6.2.1. Objetivo 1. Identificar la información relevante en los procesos auditores y los medios idóneos para la recolección de evidencia digital que permita tener un conocimiento claro de la situación evidenciada.

Unos requerimientos claramente definidos ayudan a que el diseño, desarrollo e implementación de un procedimiento o herramienta ofrezca las funcionalidades requeridas y por tanto garanticen que las acciones ejecutadas conlleven al logro del objetivo.

Esta etapa es importante ya que del análisis de la situación actual y del estudio preliminar que de esta información se realice, se desprenden las condiciones, controles y situaciones que deben evaluarse, crearse o mejorarse para garantizar que las pruebas recibidas o recaudadas, basadas en evidencia digital, presten el mérito suficiente para asegurar que las situaciones evidenciadas y reportadas ilustren de manera suficiente y clara los hechos materia de evaluación.

Se presentan 4 actividades consecutivas que se desarrollarán para obtener los insumos que den una idea clara del panorama actual y formar una base de estudio y análisis para detallar cada uno de los aspectos a mejorar, suprimir o crear dentro del procedimiento a implementar.

- Estudio de normas relacionadas con control fiscal y la norma ISO 27037:2012.
- Entrevistas para conocer los procedimientos, herramientas y riesgos existentes en los procesos.
- Establecer los tipos de información requerida como soporte dentro de un proceso o auditoría de acuerdo con las pruebas realizadas.

- Organizar resultados obtenidos para establecer información y medios óptimos.

6.2.2. Objetivo 2. Establecer los pasos, medios y responsables de la cadena de custodia para garantizar la protección, confiabilidad, integridad y salvaguarda de la evidencia digital obtenida en el proceso auditor.

Con la información anteriormente obtenida, relacionada con la forma en que actualmente se solicita, recibe y guarda la información contenida en medios electrónicos o digitales, se ejecutará un análisis de los medios y los riesgos que se originan por la falta de un procedimiento oficialmente implementado con controles, responsables y actividades claramente establecidas para garantizar la obtención y conservación de evidencia digital que pueda ser usada en cualquier etapa de la auditoría y un posible proceso de responsabilidad fiscal.

Las actividades que a continuación se relacionan, permitirán definir los pasos y actividades que deben ejecutarse cuando se está realizando una auditoría gubernamental en la cual se debe obtener pruebas basadas en evidencia digital de la entidad auditada.

- Analizar la pertinencia y confiabilidad de los medios disponibles para la salvaguarda de la evidencia digital.
- Identificar los lugares apropiados para almacenar evidencia digital.
- Configurar los pasos, medios e identificación necesaria para la evidencia digital recaudada que permita una correcta y adecuada identificación y organización.
- Organizar resultados para establecer pasos, medios y responsables del almacenamiento y custodia de información.

6.2.3. Objetivo 3. Formalizar las herramientas de software idóneas para el análisis y uso de la evidencia digital en el desarrollo de pruebas de auditoría, orientada a obtener resultados claros, confiables y que revelen la realidad de lo observado.

Con los pasos definidos para la obtención, recepción y custodia de la información obtenida en medios digitales, se hace necesario establecer los métodos necesarios para hacer un uso correcto de la misma con el fin de garantizar que las pruebas obtenidas y por tanto, los datos en ellas contenidos, sean manipulados adecuadamente para no afectar la integridad, disponibilidad, autenticidad y procedencia de la misma.

Se debe contar con la identificación completa y precisa de cada archivo recibido con el fin de que cada proceso que haga uso de información cuente con la seguridad

necesaria para determinar que esta corresponde a la situación evidenciada y contiene los datos que la entidad auditada procesa.

Las actividades, a continuación listadas, buscan determinar los métodos o pasos que debe tener en cuenta el profesional y/o especialista que evaluará los datos y presentará el informe correspondiente que permita determinar si la entidad examinada procede conforme a lo establecido en la normatividad colombiana que se encontraba vigente para las fechas evaluadas por el órgano de control.

- Estudiar las herramientas con que dispone la Contraloría General de la República para análisis de información.
- Analizar herramientas de acceso público y libre para la obtención de información electrónica y su análisis.
- Establecer las herramientas a utilizar, de acuerdo con el tipo de información analizada.
- Establecer instrucciones de análisis de información conformadas por pasos claros y precisos, de acuerdo con el tema de análisis y auditoría o prueba realizada.
- Organizar resultados para definir las herramientas a usar y procedimientos a establecer en el análisis de información.

6.2.4. Objetivo 4. Verificar, mediante la ejecución de una prueba piloto, la efectividad y eficiencia de los procedimientos, herramientas y pasos establecidos para garantizar la confiabilidad e idoneidad de la evidencia digital recaudada

Antes de la ejecución del presente objetivo, se debe contar con un compendio de pasos que comprenden la recolección o recepción de pruebas soportadas en evidencia digital, su adecuado almacenamiento y la metodología que se debe seguir para realizar los análisis correspondientes sin afectar la seguridad de los datos contenidos.

Para verificar que lo obtenido hasta el momento cumple con los objetivos y los fines esperados con el desarrollo del presente proyecto, es necesaria la ejecución de una prueba piloto que permita definir su funcionalidad y, mediante la retroalimentación de los auditores que las ejecuten, establecer los ajustes correspondientes que conllevan a un procedimiento ajustado a la normatividad y funciones de la Contraloría General de la República.

Las actividades presentadas buscan poner en ejecución el procedimiento preliminarmente diseñado y, mediante el seguimiento de los actores involucrados en el desarrollo del proyecto, determinar las observaciones y recomendaciones que se deban poner en práctica para ajustar los pasos y establecer una metodología que permita contar con evidencia digital probatorio adecuada y pertinente para el uso de la Contraloría General de la República en sus diferentes procesos y etapas.

- Confirmar que la evidencia digital recolectada dentro de una prueba de auditoría, corresponde a la información requerida para ser analizada de acuerdo con el procedimiento de auditoría.
- Evaluar el estado de almacenamiento y conservación de la evidencia recaudada, mediante pruebas de localización y lectura de los archivos digitales recolectados.
- Confrontar los resultados de los análisis obtenidos con las herramientas especificadas en el presente proyecto, con los resultados que el auditor recolecta por los medios tradicionales.
- Ajustar los pasos, medios, herramientas y/o procedimientos establecidos de acuerdo con los resultados obtenidos en la prueba realizada para cada una de las etapas anteriores.

6.2.5. Objetivo 5. Diseñar un procedimiento para la recolección, cadena de custodia y uso de la evidencia digital obtenida a partir de la práctica de pruebas de auditoría.

Una vez se haya ajustado el procedimiento y se pueda confirmar que la metodología diseñada permite recaudar, almacenar y utilizar la información digital o electrónica obtenida como acervo probatorio en una auditoría, se generará el procedimiento que será presentado a las instancias correspondientes para su implementación en caso de ser aprobada.

Las actividades a desarrollar en esta etapa buscan generar el documento final con la información que debe contener el procedimiento estableciendo los diferentes componentes para su correcta aplicación y seguimiento.

Ejecutadas estas actividades se procede a entregar el documento final a los directivos para que sea evaluado y conforme a la normatividad y políticas de la Contraloría General de la República se establezca si el mismo puede ser implementado.

- Acopiar la información y resultados obtenidos.
- Consolidar los resultados obtenidos en las diferentes fases.
- Identificar los responsables de las diferentes etapas del procedimiento.
- Organizar y estructurar el procedimiento de recolección, cadena de custodia y uso de evidencia digital.

7. RECOLECCIÓN DE EVIDENCIA DIGITAL

7.1. CONTROL FISCAL COLOMBIANO

El Control Fiscal hace referencia a la vigilancia de la gestión fiscal realizada por parte de la administración y de los particulares o entidades que manejan fondos o bienes de la Nación.

Este control, en Colombia, es ejercido por la Contraloría General de la República, como máximo órgano de control fiscal, de acuerdo con el artículo 267 de la Constitución Política, por tanto, tiene la obligación de realizar los procedimientos necesarios para examinar el uso de los recursos públicos del orden nacional que realicen las entidades de la administración o particulares.

La Contraloría General de la República, planea los procesos de vigilancia fiscal que se realizarán durante cada vigencia, de acuerdo con parámetros técnicos de selección, así como de los lineamientos jurídicos y funciones establecidas en la legislación colombiana. Esta planeación se enmarca en el Plan de Vigilancia y Control Fiscal, el cual tiene como procedimiento de aplicación la Guía de Auditoría, creada por la Contraloría para la ejecución de sus procesos auditores y que contiene los lineamientos, instrucciones y responsables en las diferentes etapas del proceso auditor.

Este plan, el cual contiene información como las entidades a examinar, los objetivos del proceso auditor que se adelantará, los términos para su desarrollo y los grupos encargados de hacerla, es comunicado a cada Gerencia Departamental Colegiada para que adelante los distintos procesos que se hayan definido y correspondan a su jurisdicción.

Los grupos determinados para este fin se encargarán de establecer los procedimientos de auditoría necesarios para cumplir con los objetivos establecidos dentro del programa de auditoría creado. Dentro del desarrollo de procedimientos es necesario verificar, acorde con la normatividad vigente aplicable a la fecha del ejercicio auditor, el cumplimiento de las funciones y políticas establecidas por el Estado para una entidad, institución o sujeto de control fiscal en particular.

Como resultado de estos procesos, es posible encontrar situaciones o condiciones que permiten inferir que el sujeto auditado no ha cumplido sus funciones de acuerdo con las normas establecidas, razón por la cual debe comunicarse la observación al ente sobre los eventos y pruebas que permiten determinar que dicha situación no se apega a la Ley.

Si no es posible que lo observado se descarte como una situación con deficiencias por parte del vigilado, se determina un hallazgo con posible incidencia fiscal (cuando

se establece que se ha causado un daño al erario público), el cual debe configurarse conforme a los requisitos y condiciones establecidas en la Guía de Auditoría dispuesta por la Contraloría General de la República y soportado en evidencia recolectada por el equipo auditor durante el examen realizado.

Todo hallazgo con presunta incidencia fiscal puede generar un proceso de responsabilidad fiscal adelantado y tramitado por la Contraloría General de la República con el fin de demostrar el daño fiscal causado, los responsables de que el daño evidenciado se haya materializado y la cuantía del mismo, en aras de lograr el resarcimiento del daño y la recuperación de los recursos públicos afectados.

Toda evidencia, dentro del proceso auditor y dentro de un posible proceso de responsabilidad fiscal, debe ser suficiente, confiable y relevante para la condición que se pretende demostrar.

7.2. APLICACIÓN DE LA NORMA ISO 27037:2012

Esta norma o modelo internacional, establece directrices o procedimientos para la recolección, análisis y preservación de la evidencia digital guardada y conservada en distintos dispositivos de almacenamiento electrónico u óptico.

En el desarrollo del presente proyecto se tendrá en cuenta los aspectos de la norma, relacionados con la identificación y adquisición de soportes de auditoría en medio electrónico o digital que sirva como evidencia dentro de un proceso auditor con el fin de garantizar la eficiencia de la misma como soporte para demostrar una situación, detectada durante la ejecución de un proceso auditor en una entidad examinada, y que no cumple los lineamientos legales y jurídicos establecidos para ella.

Se tendrá en cuenta específicamente lo relacionado con la recepción e identificación de información o evidencia digital suministrada por la entidad vigilada con el fin de contar con información consistente, integra y confiable que pueda ser valorada como prueba adecuada, suficiente y relevante en un proceso de responsabilidad fiscal.

7.3. PROCEDIMIENTOS, HERRAMIENTAS Y RIESGOS

El levantamiento de la información se realiza sobre la muestra correspondiente a un grupo auditor de la Gerencia Departamental Colegiada del Valle del Cauca que actualmente se encuentre desarrollando una auditoría. Para esto, se ha seleccionado el proceso auditor adelantado a una Entidad Promotora de Salud (EPS) en el departamento del Valle del Cauca.

El grupo auditor asignado a la realización de este proceso se compone de siete (7) profesionales con los siguientes perfiles: dos (2) abogados, dos (2) contadores públicos, un (1) economista, un (1) administrador de empresas y un (1) ingeniero de sistemas.

7.3.1. Procedimientos y Herramientas utilizados en auditoría. Se realiza entrevista personal a cada uno de los profesionales que conforman el grupo de acuerdo con las preguntas configuradas en el formato establecido (Ver anexo B).

Cada una de las preguntas establecidas previamente en el formato creado, es contestada por los profesionales desde su perfil profesional, su experiencia, la naturaleza de la entidad auditada (EPS) y los objetivos previamente establecidos en el Plan de Vigilancia y Control Fiscal.

Con las respuestas de los entrevistados se generan los resultados correspondientes a los procedimientos, herramientas para realizar su labor auditora y la forma en la cual la información es entregada por parte del ente examinado.

Los procedimientos más utilizados, para la solicitud de información son:

- Requerimiento de información por medio de documento escrito, en el cual se especifica la información requerida, la estructura de la información, formato de los archivos y la vigencia de los eventos que fueron registrados.
- Solicitud mediante correo electrónico de la información requerida con las especificaciones descritas en el ítem anterior.

La información requerida por el grupo auditor, contenida en medios digitales ya sean archivos electrónicos pertenecientes a la entidad, reportes de información obtenidos a partir de los diferentes activos de software del ente auditado (sistemas de información y/o aplicaciones de software), corresponde a registros que el ente auditado crea y procesa en relación con sus labores administrativas y financieras.

Las herramientas de software utilizadas por los diferentes profesionales para el análisis son las siguientes:

Tabla 1. Herramientas de software para análisis de información digital

Profesional entrevistado	Herramienta utilizada
Abogados	Microsoft Excel
Contadores Públicos	Microsoft Excel
Economista	Microsoft Excel
Administrador de Empresas	Microsoft Excel
Ingeniero de Sistemas	SQL Server Express, IDEA, Microsoft Excel

Fuente: Entrevistas aplicadas por el autor del proyecto

Como se observa en el cuadro, a excepción del Ingeniero de Sistemas, la herramienta más utilizada para los análisis de datos contenidos en información almacenada en medios digitales es Microsoft Excel.

En cuanto a la información entregada por la Entidad auditada, en respuesta a los requerimientos realizados, la misma es suministrada generalmente en medios ópticos como CD o DVD y también puede ser suministrada en archivos electrónicos adjuntos a mensajes de correo electrónico.

La información se recibe por parte de los miembros del grupo auditor, acompañada de un documento suscrito por la entidad, relacionando únicamente la información que se entrega y el requerimiento al cual se está dando cumplimiento.

Se observa también que la información recibida en medios ópticos viene rotulada en la cara del CD o DVD dispuesto para escritura con marcadores rotuladores, con la información del número de oficio (documento impreso con el cual se realiza el requerimiento por parte del equipo auditor).

La información recibida, en algunos casos se genera una copia para su análisis y manejo y en otras ocasiones, se sigue leyendo desde el medio original (CD o DVD recibido).

El almacenamiento de la información recibida en medios ópticos, se realiza archivando los mismos en su empaque original, sin relacionar su origen, tipos de datos contenidos o características de ubicación para su posterior localización.

Cuando la información se entrega como un archivo adjunto a un mensaje de correo electrónico, la misma se remite con un mensaje indicando la información y el requerimiento contestado. No se realiza procedimientos para generar una copia que sea almacenada en un medio físico que permita su archivo y salvaguarda.

7.3.2. Riesgos identificados en la entrevista. Analizadas las respuestas presentadas por los profesionales entrevistados, se puede observar la presencia de los siguientes riesgos:

- Pérdida de información por almacenamiento inadecuado.
- Pérdida de información de archivos adjuntos en el correo electrónico por no realizar copia de los mismos.
- Modificación involuntaria de datos almacenados en archivos grabados en medios ópticos con opción de escritura.
- Afectación a la autenticidad de los datos por falta de parámetros que aseguren el origen de los archivos entregados por la entidad auditada.

- Análisis de Datos en herramientas como Excel que no permite la importación de archivos planos o bases de datos con más de 1.048.576 registros en sus últimas versiones.
- Ausencia de datos cronológicos de los archivos recibidos para confirmar el momento de generación del mismo.

Estos riesgos pueden afectar la integridad y la irrefutabilidad (no repudio, no rechazo) de la información recibida.

7.4. TIPOS DE INFORMACIÓN REQUERIDA COMO SOPORTE

De acuerdo con la entrevista realizada, la información requerida por los diferentes profesionales integrantes del equipo que realiza el examen es:

Tabla 2. Información requerida en el proceso auditor

Profesional entrevistado	Información requerida como insumo
Abogado 1	Relaciones de contratos reportadas por aplicaciones de software
Abogado 2	Información Contractual, reportada por los sistemas de información institucionales.
Contador Público 1	Información contable, cuentas por pagar, cuentas por cobrar, balances, informes generados por los sistemas contables implementados.
Contador Público 2	Registros de cuentas contables, balances, presupuestos, reportes del software contable o aplicaciones utilizadas para el registro contable y financiero.
Economista	Registros de afiliados y beneficiarios de los planes de promoción y prevención
Administrador de Empresas	Red de prestadores de la EPS. Reportes de afiliados.
Ingeniero de Sistemas	Reportes generados en archivos planos de afiliados en las vigencias a auditar, reportes de recobros solicitados a FOSYGA de las tecnologías en salud no incluidas en el POS, Base de Datos Única de Afiliados de la EPS.

Fuente: Entrevistas aplicadas por el autor del proyecto

La información requerida por los abogados, contadores públicos, economista y administrador de empresas, es solicitada en formato de Excel ya que es la herramienta que utilizan para realizar filtros, ordenaciones, conteos, y otros análisis necesarios en los procedimientos establecidos de acuerdo con los objetivos planeados en la auditoría planeada.

El Ingeniero de Sistemas realiza solicitudes de información en archivos planos y de información que contiene cantidades de registros que sobrepasan el límite establecido en la hoja de cálculo mencionada. Los análisis realizados por este

profesional consisten en consultas de información entre diferentes fuentes, en búsqueda de coincidencias, presuntas duplicidades de afiliados en reportes en los cuales no deben existir, entre otros relacionados con búsquedas y consultas masivas de información para lo cual se hace uso de instrucciones SQL.

En todos los casos, la información requerida para el desarrollo de los procedimientos de auditoría ejecutados por los profesionales, y que involucra evidencia en medios digitales, se puede clasificar en:

- Información generada por los sistemas de información o aplicaciones de software institucionales.
- Archivos electrónicos generados por personas, almacenados en medios electrónicos como discos duros internos, discos duros externos y unidades de almacenamiento extraíble USB.
- Archivos electrónicos generados por personas, almacenados en medios ópticos.
- Archivos electrónicos remitidos como adjuntos en correos electrónicos.

Los archivos requeridos dentro de los procesos auditores son solicitados en formato compatible con Microsoft Excel o como archivos planos para poder ser abiertos con la aplicación de software Microsoft Excel, IDEA o los DBMS SQL Server Express o PostgreSQL.

Los archivos que se reciben en formato PDF, son nuevamente solicitados a la entidad auditada en uno de los formatos anteriormente mencionados con el fin de garantizar la confiabilidad de la misma y la irrefutabilidad de la fuente de la cual proviene, sin embargo, se observa ausencia de mecanismos que fortalezcan esta última característica.

7.5. RESULTADOS

Una vez acopiadas las respuestas de la entrevista y analizados los aspectos relacionados con los procedimientos, herramientas y tipos de información utilizada por los profesionales en la ejecución de una auditoría gubernamental a una Entidad, se presenta a continuación, los pasos o actividades a desarrollar en la fase del procedimiento relacionada con la recolección de evidencia digital.

7.5.1. Requerimientos de la información solicitada. La información solicitada por los auditores como evidencia a ser analizada, para determinar el cumplimiento o no de las funciones establecidas en la Ley por parte de la entidad vigilada, deberá contar con una certificación emitida por el propietario de la misma, independiente

del medio de origen y/o fuente del reporte, que garantice su origen, la autenticidad y confiabilidad de la misma.

Toda solicitud oficial emitida por el equipo auditor al ente vigilado, con el fin de solicitar información en medios digitales (archivos electrónicos, reportes emitidos por productos de software institucionales, archivos digitales, y otros relacionados), deberá requerir una relación de cada uno de los archivos suministrados, que contenga como mínimo los siguientes datos identificadores (metadatos):

- Nombre completo del archivo electrónico, incluyendo su extensión.
- Tamaño en bytes que ocupa el archivo en el medio de almacenamiento suministrado (CD, DVD o mensaje de correo electrónico).
- Fecha de creación del archivo suministrado, incluyendo hora.
- Código HASH o huella digital utilizando el algoritmo criptográfico que se determine por parte de la USATI.

Si la información se presenta en un medio óptico (CD o DVD) debe venir rotulada, en la cara del medio dispuesta para ello, con los siguientes datos:

- Número de oficio de solicitud del grupo auditor.
- Fecha de solicitud del grupo auditor.
- Número de oficio de respuesta de la entidad auditada.
- Fecha de respuesta de la entidad auditada.

7.5.2. Recepción de la información solicitada. La información entregada por la entidad en respuesta a un requerimiento de información en medios digitales debe contener la relación de archivos con las características de identificación mencionadas en el punto anterior. La relación requerida debe presentarse en medio impreso para los medios ópticos y en un archivo electrónico adjunto para los correos electrónicos. De no contar con esta relación, debe devolverse la información al ente auditado para generar la relación correspondiente y formalizar su entrega y recepción a cabalidad.

Si la información se presenta en un medio óptico (CD o DVD), se debe verificar que contenga la identificación rotulada en su cara conforme a las indicaciones establecidas. En caso de no contar con esta identificación, el equipo auditor debe realizarla. Adicionalmente, debe validarse que los metadatos (datos identificadores) correspondan con los informados por la entidad en la entrega formal.

Adicionalmente, la información debe ser leída en un equipo de cómputo para garantizar que no se presentan inconvenientes de lectura y que la misma ha sido generada, grabada y/o transmitida correctamente.

7.5.3. Disposición de la información recibida en auditoría. Toda la información recibida debe ser catalogada en el formato que se establece para el inventario de información o evidencia digital recibida durante el proceso auditor (Ver anexo B).

Cada uno de los medios de almacenamiento de información recibido y verificado, se debe identificar por medio de la referencia establecida por la Guía de Auditoría para el oficio de respuesta emitido por la entidad vigilada.

Los medios ópticos o digitales recibidos deben ser mantenidos en sus empaques originales entregados por la entidad vigilada.

7.5.4. Medios Requeridos para recibir evidencia solicitada. Los equipos auditores, para el correcto desarrollo de sus procedimientos de auditoría, requiere para analizar la gestión y desempeño de la entidad sujeto de análisis, de información que pertenece a dicha entidad y la cual contiene registros de las actuaciones que ha llevado a cabo. Esta información puede ser solicitada en medio físico o electrónico, dependiendo de las directrices legislativas, del método de archivo y del tipo de información.

La información recibida, únicamente será admitida en medios ópticos como CD o DVD, o como un archivo adjunto por medio de correo electrónico.

Toda la información solicitada en medio digital o electrónica, por parte del equipo auditor, únicamente será válida en los siguientes medios, formatos y características:

- La información que se transmite por un medio de comunicación como el correo electrónico, deberá ser validada con los datos identificativos requeridos en la solicitud. En el caso de no corresponder con estos valores identificadores, se deberá devolver a la entidad remitente y requerir su corrección.

Si la información es correcta, la misma será grabada o archivada en un disco óptico, que puede ser DVD o CD dependiendo del tamaño, junto con los valores identificativos de los archivos.

Cada solicitud debe corresponderse con uno de estos medios, es decir, debe existir un CD o DVD por cada envío de información de una solicitud realizada por el equipo auditor.

- La información recibida directamente en CD o DVD, deberá ser comparada con sus datos identificadores, y validado su correcto funcionamiento en un equipo de cómputo.

De igual manera que un correo electrónico, de no corresponder la información con su identificación solicitada, será devuelta al remitente para su corrección.

- Para el caso de la información correspondiente a documentación que deba ser analizada en un medio digital, se aceptarán archivos en formato PDF, TIFF o JPEG.

- Para los archivos que contienen información que requiere de consultas de comparación, búsqueda o filtros, los formatos admitidos corresponden a hojas de cálculo en Excel, archivos planos separados por coma, archivos planos separados por punto y coma y archivos planos separados por tabulaciones.

- Toda evidencia digital que sirva como soporte para un hallazgo con incidencia fiscal, debe ser almacenado en un medio óptico como CD o DVD, debidamente rotulado y enviado para su almacenamiento en custodia. El medio óptico mencionado estará disponible para consulta o práctica de pruebas adicionales requeridas dentro de una indagación preliminar o proceso de responsabilidad fiscal.

8. CADENA DE CUSTODIA PARA MATERIAL DIGITAL

8.1. MEDIOS DISPONIBLES PARA ALMACENAR EVIDENCIA DIGITAL

En la actualidad, la Gerencia Departamental Colegiada Valle del Cauca de la Contraloría General de la República cuenta con los siguientes medios disponibles para el almacenamiento físico de la evidencia digital recaudada como material probatorio de los procedimientos de auditoría adelantados:

- Medios ópticos como CD o DVD.
- Discos Duros.

La Gerencia Departamental posee, dentro de su inventario de activos, un repositorio en el servidor de archivos para el almacenamiento de la información que soporta los distintos procesos auditores, sin embargo, la misma es susceptible de ser afectada por problemas eléctricos o de manipulación voluntaria o involuntaria de los funcionarios que cuentan con acceso a dicho repositorio, lo cual deja expuesta la prueba a contaminación y posible destrucción o pérdida de los datos ahí almacenados.

Por otro lado, la información documental y probatoria de los diferentes procesos auditores es archivada, conjuntamente con la documentación física generada y recaudada durante el ejercicio auditor, en un archivo físico central en el cual se almacenan conjuntamente las carpetas de cartón con los distintos documentos físicos y los medios ópticos que contienen los documentos electrónicos grabados en ellos. No obstante, dicha disposición se realiza en cajas diseñadas para archivo físico que no garantizan la protección y conservación, en el tiempo, de los medios ópticos archivados exponiéndose los mismos a daños y estropeos causados por su manipulación al mover una caja o extraer una carpeta de cartón, conllevando con esto a estropear la prueba recaudada toda vez que se tendría un medio óptico con datos no reconocibles por las unidades lectoras y por tanto irrecuperables como soporte probatorio apropiado.

Como se puede observar, la disposición actual de los archivos electrónicos almacenados en medios físicos como discos duros y/o servidores y aquellos que se archivan en medios ópticos, no permite garantizar una preservación de los datos almacenados en ellos que garantice su correcta recuperación en un futuro en el cual sea requerido como soporte para demostrar el incumplimiento de una directriz, obligación o norma legislativa y de esta forma obtener la recuperación de los recursos detectados como daño causado al erario público por la situación evidenciada.

8.2. REQUERIMIENTOS PARA ARCHIVO DE EVIDENCIA DIGITAL

Tal como se evidencia en la etapa de recolección, la información correspondiente a la evidencia digital recaudada como soporte de un hallazgo que permita evidenciar la ocurrencia de acciones contrarias a la normatividad y ley colombiana, se almacenará en medios ópticos debidamente rotulados, que pueden ser CD o DVD.

Con el fin de preservar la integridad de este medio, es necesario que el mismo se almacene o archive en un espacio diseñado para su ubicación y preservación. Se debe tener en cuenta los siguientes requerimientos para su adecuado almacenamiento físico:

- Este tipo de medios de almacenamiento de información requieren de un espacio que conserve la temperatura adecuada, especificada por cada empresa fabricante.

- El espacio asignado debe ser un lugar con una adecuada ventilación para evitar la acumulación de polvo.

- Cada uno de los medios de almacenamiento (CD o DVD), debe ser empaquetado en sobres de vinil de transparencia cristalina para garantizar su protección a rayones y su identificación.

- Los medios de almacenamiento a adquirir deben ser aquellos que presentan una vida útil superior a los términos establecidos por la Unidad de Archivo y Correspondencia de la Contraloría General de la República para la permanencia en archivo de la información de los procesos auditores (términos establecidos en la tabla de retención documental de la Contraloría General de la República).

Es de anotar que la labor de archivo de la información debe corresponder a un funcionario que tenga conocimientos en gestión de archivo y correspondencia; además, este funcionario debe tener conocimientos relacionados con el manejo adecuado de medios ópticos.

El espacio determinado para el archivo de los medios ópticos entregados por los equipos auditores al finalizar sus asignaciones, será el dispuesto por el Presidente Colegiado de la Gerencia Departamental para este fin y contará con los requerimientos necesarios de acuerdo con las especificaciones establecidas por el fabricante para su correcta conservación y salvaguarda.

8.3. IDENTIFICACIÓN DE EVIDENCIA DIGITAL PARA SU CUSTODIA

Acorde con lo establecido para identificar los medios de almacenamiento, en la fase de recolección de información solicitada, la evidencia digital grabada en medios ópticos debe contener la siguiente información rotulada en la cara del CD o DVD, dispuesta para este propósito:

- Número de oficio de solicitud del grupo auditor.
- Fecha de solicitud del grupo auditor.
- Número de oficio de respuesta de la entidad auditada.
- Fecha de respuesta de la entidad auditada.

Internamente, la información grabada en el medio de almacenamiento debe contener, además de los datos requeridos por el grupo auditor, los datos identificadores (metadatos) de cada uno de los archivos o documentos electrónicos grabados que garantizan su autenticidad e irrefutabilidad en cuanto a su procedencia, propiedad y autoría de los mismos.

Tal como se estableció, cada medio de almacenamiento debe corresponder a una solicitud de información como máximo. Es posible que, por el volumen de la información requerida, se deba utilizar más de un medio de almacenamiento (dos o más CD o DVD) para dar respuesta a un requerimiento de información.

Adicionalmente, la información recibida en la Entidad debe contar con un número de identificación interno, a nivel de archivo de medios digitales, que permita su ubicación y fácil localización en caso de ser requerida por un funcionario en el desarrollo de sus funciones dentro de una indagación preliminar o proceso de responsabilidad fiscal.

8.4. ALMACENAMIENTO Y CUSTODIA DE EVIDENCIA DIGITAL

Con el fin de preservar la información que compone la evidencia digital recaudada como sustento probatorio dentro de un proceso auditor, se definen los siguientes pasos a cumplir, de manera obligatoria, por parte de los equipos auditores una vez terminadas las actuaciones en las entidades asignadas:

8.4.1. Identificación y embalaje de medios de almacenamiento. Todos los medios de almacenamiento (CD o DVD), recibidos o generados dentro del proceso auditor, deben venir debidamente rotulados identificando como mínimo los siguientes datos:

- Número de oficio de solicitud del grupo auditor.

- Fecha de solicitud del grupo auditor.
- Número de oficio de respuesta de la entidad auditada.
- Fecha de respuesta de la entidad auditada.

Cada uno de los medios de almacenamiento debe ser embalado en sobres de vinil de transparencia cristalina, que permita ver su correspondiente rotulo de manera clara. La cantidad de CD o DVD, debe corresponder con la relacionada en el formato de inventario de evidencia digital recibida (Anexo B), que se adjuntará al oficio de entrega al archivo de evidencias digitales.

8.4.2. Recepción de medios de almacenamiento. El líder del equipo auditor, una vez terminada la auditoría, entregará al funcionario asignado para la gestión y administración del archivo de evidencia digital los medios de almacenamiento óptico (CD, DVD) que haya recibido o generado dentro del proceso auditor y que correspondan a evidencia en medio electrónico o digital, recolectada como soporte de los procedimientos.

La entrega de la información digital, debidamente embalada, debe realizarse mediante oficio remisorio que deberá relacionar:

- Auditoría realizada.
- Entidad auditada.
- Vigencia auditada.
- Cantidad de CD o DVD entregados a archivo de evidencia digital.

El oficio y los medios de almacenamiento deberán estar acompañados de una copia del inventario de evidencia digital recibida durante el proceso auditor, debidamente diligenciado en su totalidad y firmado por el líder del equipo auditor. Se entregará, por parte del líder, una (1) copia en físico y una (1) copia en archivo electrónico.

El paquete embalado será recibido y verificado por el funcionario asignado al archivo de evidencia digital quien comprobará la información recibida, la cantidad de medios entregados por el líder del equipo auditor, la correcta identificación de los medios y el embalaje de los mismos.

Si la revisión realizada en el momento de la entrega presenta inconsistencias, la misma será devuelta al equipo auditor para que realice las correcciones a que haya lugar. En caso contrario, el funcionario dará su visto bueno de conformidad con la información y medios recibidos, indicando la fecha y hora de la entrega correcta.

El oficio remisorio deberá contar con su correspondiente número de radicación generado por el software de uso oficial de la Contraloría General de la República, para la gestión de la correspondencia.

8.4.3. Disposición y ubicación de medios de almacenamiento. Una vez recibidos a conformidad los medios de almacenamiento, el funcionario encargado de archivarlos, realizará el registro del paquete en el medio informático dispuesto para tal fin (hoja de cálculo, aplicación o software de inventario).

El registro realizado permitirá asignar un código interno de identificación del conjunto de medios de almacenamiento y una referencia geográfica de ubicación dentro del espacio determinado para la disposición de dichos medios.

El medio informático seleccionado para el registro de los medios de almacenamiento recibidos en el archivo correspondiente, deberán permitir el registro de la fecha de recibo y/o generación de los medios magnéticos, con el fin de tener un control sobre el tiempo de vida útil esperado para los CD o DVD recibidos.

Una vez recibidos, se deberá realizar una copia de los mismos como respaldo en caso de pérdida o daño de los medios o la información almacenada en ellos.

Estos medios se encontrarán a disposición de los funcionarios interesados o asignados a procesos que se generen a partir de los hallazgos detectados. Para esto, deberá contar con el respectivo documento, firmado por el directivo correspondiente, quien, en conjunto con el funcionario solicitante, serán los responsables de la salvaguarda y cuidado de los medios requeridos durante el tiempo del préstamo.

Se recomienda, salvo situaciones que lo ameriten, un tiempo máximo de dos (2) días de préstamo. Este tiempo es necesario para que el funcionario o funcionarios asignados realicen una copia de los archivos contenidos en un medio distinto con el fin de salvaguardar el medio original que corresponde a la prueba generada o entregada por la entidad examinada.

9. HERRAMIENTAS PARA ANALISIS DE INFORMACIÓN DIGITAL

9.1. PRODUCTOS DE SOFTWARE PARA ANÁLISIS DE INFORMACIÓN

Con el fin de realizar los análisis correspondientes para obtener resultados en las pruebas de auditoría que tienen como soporte los datos e información almacenada en medios digitales, es necesario contar con herramientas que sean confiables y cuyos procedimientos garanticen que los resultados obtenidos puedan ser utilizados como acervo probatorio en el momento de presentarlos ante la entidad examinada, así como servir de sustento probatorio dentro de un proceso de responsabilidad fiscal que se adelante como resultado de un hallazgo con posible incidencia fiscal.

Gran parte del éxito de un proceso basado en este tipo de pruebas consiste en que este material recaudado sea obtenido guardando y conservando sus características de integridad e irrefutabilidad ante el dueño o creador de la información.

La otra parte consiste en que las pruebas realizadas, se ejecuten sobre el material debidamente recaudado, pero manteniendo unos estándares de calidad que puedan garantizar la idoneidad de la prueba, así como su suficiencia y la pertinencia dentro de los procesos que la requieran.

Para garantizar estos aspectos, necesarios dentro de un proceso que requiera el uso de material probatorio basado en pruebas de auditoría sobre material digital o evidencia electrónica, se realiza un estudio para obtener un listado de las herramientas disponibles en la Gerencia Departamental Valle del Cauca y en el entorno de las herramientas informáticas de libre distribución y uso (software libre).

9.1.1. Software propiedad de Contraloría General de la República. La Gerencia Departamental Valle del Cauca de la Contraloría General de la República, de acuerdo con los lineamientos del Nivel Central, tiene a su disposición las siguientes herramientas para el análisis de información en medios digitales:

- Microsoft Excel.
- Microsoft Access.
- IDEA.

Estas herramientas tienen la licencia correspondiente, adquirida por la Contraloría General de la República para uso de los funcionarios dentro de las actividades de auditoría requeridas.

9.1.2. Software de uso libre. Por otra parte, en cuanto a herramientas de software libre se refiere, se encuentran los diferentes DBMS (Sistemas Gestores de bases de datos) que permiten, además de la creación y gestión de bases de datos, de la importación de archivos digitales como grandes tablas, archivos planos o bases de datos en diferentes formatos, con el fin de realizar consultas mediante la creación de vistas o el uso de sentencias en el lenguaje SQL para detectar inconsistencias, realizar cálculos o presentar estadísticas y comportamientos de acuerdo con la información analizada.

Un ejemplo de estos productos es:

- SQL Server Express.
- PostgreSQL.
- MySQL.

Adicionalmente, existen herramientas que permiten calcular el código hash o huella digital de un archivo electrónico con el fin de obtener una identificación que permita asegurar la integridad de la información almacenada y que el medio tomado como fuente de análisis no ha sido alterado y permanece fiel a lo reportado por la Entidad auditada.

Entre las aplicaciones o herramientas que permiten calcular el código hash de los archivos electrónicos, que son compatibles con el sistema operativo Windows instalados y usado en la Contraloría General de la República y, además, corresponden a software de uso libre, se cuenta con Hashmyfiles y Multi Hasher que son productos de software gratuitos que permiten calcular el código hash de archivos electrónicos, utilizando los algoritmos criptográficos: MD5, SHA-1, CRC32, SHA-256, SHA-512 y SHA-384.

9.2. EVALUACIÓN DE SOFTWARE PARA ANÁLISIS DE DATOS

De acuerdo con el inventario de software obtenido, se realiza el estudio de las ventajas y desventajas que las herramientas disponibles actualmente presentan en relación con la objetividad y efectividad de los análisis requeridos, así como la disponibilidad de las mismas para efectuar pruebas con la oportunidad exigida por los procedimientos, lineamientos y normatividad establecida para la realización de auditorías en la Contraloría General de la República.

9.2.1. Microsoft Excel. Esta herramienta desarrollada por la empresa Microsoft y parte del paquete ofimático Microsoft Office, es una hoja de cálculo que permite realizar operaciones con datos organizados en tablas, tales como operaciones matemáticas, operaciones de comparación, búsqueda, lógicas, entre otras.

Cada archivo de Excel se conoce como Libro y puede componerse de una o más hojas de cálculo.

Este producto de software, además de la realización de cálculos y otras operaciones con los datos almacenados, tiene la opción de importar archivos que se encuentren en otros formatos diferentes al de la hoja de cálculo de Excel, tales como texto, Access, Web, SQL Server y otras fuentes.

La Contraloría General de la República ha adquirido equipos de cómputo para los funcionarios de las diferentes gerencias departamentales y cada uno de ellos viene con el paquete de Microsoft Office instalado y licenciado para la Contraloría; por esta razón, es un software que no necesita ser instalado y configurado cuando se requiera, sino que está disponible en cualquier momento.

Para la realización de búsquedas y consultas, es necesario conocer las diferentes fórmulas que vienen prediseñadas, siendo necesario en muchas ocasiones crear columnas de datos adicionales para realizar las comparaciones u operaciones requeridas por el auditor que está ejecutando el análisis de la información digital.

Por otro lado, este producto tiene una capacidad limitada de registros que puede importar (número máximo de filas disponible por hoja), lo cual se convierte en una limitante cuando se trabaja con archivos que contienen información poblacional del orden departamental o nacional, que fácilmente puede superar el número de filas disponibles (1.048.576 filas en las últimas versiones).

En el caso de operaciones aritméticas a efectuar por los contadores, administradores o cualquier funcionario que desee evaluar los cálculos de cifras contables o presupuestales de una entidad auditada, Excel se convierte en una herramienta muy importante ya que contiene diversas operaciones matemáticas que puede realizar, así como diferentes formas de presentación de datos y cifras.

Adicional a lo anterior, Excel cuenta con la función de crear gráficos o estadísticas a partir de una tabla o conjuntos de datos dentro de sus hojas, lo cual nos ayuda a realizar análisis de comportamientos o del uso y distribución de recursos financieros en una entidad.

9.2.2. Microsoft Access. Este es un sistema gestor de bases de datos (DBMS por sus siglas en inglés), que también forma parte del paquete Microsoft Office.

Esta herramienta permite también la importación de archivos en diferentes formatos para cargarlas como tablas de una base de datos, permitiendo la realización de consultas en un ambiente gráfico entre diferentes tablas para el análisis y búsqueda

de inconsistencias o coincidencias entre las fuentes de información o evidencia digital recaudada.

A diferencia de Excel, Access está orientado al trabajo exclusivo con bases de datos y además permite importar archivos con una mayor cantidad de registros.

9.2.3. IDEA. Es un software de la empresa CaseWare Analytics que permite realizar diferentes análisis sobre archivos con datos organizados como tablas o bases de datos. Esta herramienta permite importar archivos en una gran cantidad de formatos diferentes.

Según CaseWare Analytics[8], contiene más de 100 funciones de uso frecuente en las auditorías, a tan solo un clic, incluidas la Ley de Benford, identificación avanzada de duplicados aproximados usando hasta tres campos carácter, detección de omisiones, manipulación de campos, resumen, estratificación, muestreo y muchas más.

Esta herramienta de la cual, la Contraloría General de la República ha adquirido licencias de uso, puede realizar diferentes análisis y consultas a la información recaudada, y generar resultados, gráficos y estadísticas muy importantes para soportar las pruebas realizadas, así como los diferentes hallazgos que sean detectados durante el desarrollo del proceso auditor.

Para ejercer un control sobre el uso de licencias de este producto, su ingreso se realiza por medio de un token suministrado por la empresa desarrolladora y el cual debe ser actualizado y activado mediante un proceso establecido por dicha empresa. Este proceso puede generar algunas demoras si una actualización es requerida y la misma no se realice a tiempo.

9.2.4. SQL Server Express, PostgreSQL y MySQL. Estas son herramientas de software libre que, al igual que Microsoft Access, son sistemas gestores de bases de datos que permiten administrar datos organizados como tablas o bases de datos, mediante interfaces gráficas o el uso de instrucciones SQL.

La ventaja de estas herramientas es que son productos de uso libre que se pueden descargar sin costo alguno y se pueden instalar en diferentes equipos, y para el caso de postgresql y mysql, independiente del sistema operativo del computador utilizado.

[8] CASEWARE ANALYTICS. Análisis de datos IDEA. [en línea]. <http://www.casewareanalytics.com/es/products/análisis-de-datos-idea>

Se convierten en una herramienta útil en el caso de encontrarse desarrollando procedimientos de auditoría que requieran análisis de datos digitales en computadores de la entidad auditada en la cual no es posible instalar software comercial, por requerir de la adquisición de licencias como es el caso de Microsoft Access e IDEA que no vienen por defecto como parte integral de los sistemas operativos o de ediciones específicas de los paquetes ofimáticos adquiridos, como es el caso de Microsoft Office.

9.3. TIPOS DE ANÁLISIS SEGÚN INFORMACIÓN RECIBIDA

Los análisis a realizar, dependen mucho del tipo de información recibida y de los objetivos específicos que la asignación de auditoría contiene de acuerdo con la planeación que realiza el Nivel Central de la Contraloría General de la República para cada vigencia, y por tanto las herramientas requeridas pueden variar en función de los tipos de análisis.

Se evalúa la información que los auditores de la muestra requieren para la ejecución de sus procedimientos, y se determina los análisis que se desean realizar, así como las herramientas que permitirán adelantarlos.

Tabla 3. Tipos de análisis según información recibida

Tipo de información	Análisis requeridos
Relaciones de Contratos reportadas por aplicaciones de software	Estadísticas de cantidades de contratos por tipo de contratación
Información Contractual, reportada por sistemas de información	Suma de valores de la contratación
Información contable, cuentas por pagar, cuentas por cobrar, balances, informes generados por los sistemas contables implementados.	Determinar sumas, clasificar gastos, análisis de entradas y salidas, determinar porcentajes de gastos.
Cuentas, Balances, Presupuestos, reportes del software contable o aplicaciones utilizadas para el registro contable y financiero.	Seguimiento de los registros en los términos establecidos, correspondencia con otras fuentes. Porcentajes de gasto, cálculo de la disponibilidad presupuestal, después de gastos e inversión.
Registros de afiliados y beneficiarios de los planes de promoción y prevención	Cálculo de cantidades según sede. Verificar afiliados reportados por EPS con otras fuentes del Estado
Red de prestadores de la EPS. Reportes de afiliados.	Consultas Entre las dos fuentes para encontrar estadísticas de afiliados por EPS y verificar capacidad
Reportes generados en archivos planos de afiliados en las vigencias a auditar, reportes de recobros solicitados a FOSYGA de las tecnologías en salud no incluidas en el POS, Base de Datos Única de Afiliados de la EPS.	Consultas en búsqueda de afiliados existentes, recobros a afiliados a salud habilitados. Comprobación de recobros. Cruces de información en búsqueda de inconsistencias como duplicidades o fallecidos.

Fuente: Análisis realizado por el autor del proyecto

De acuerdo con la información recibida y los resultados esperados por los funcionarios auditores, se puede resumir que toda la información relacionada con cuentas, presupuesto, análisis financieros y todas aquellas en las que se encuentra involucrado un análisis de tipo contable, requieren del uso de una herramienta como Excel que permite realizar cálculos de diversos tipos y a la vez permite generar estadísticas mediante fórmulas y presentación de resultados con el uso de gráficas creadas a partir de los datos analizados.

Por otro lado, la información que requiere de análisis o búsquedas de coincidencias, consultas que requieren buscar datos de una fuente en otra, y que a su vez se encuentran en archivos de gran tamaño de registros, necesitan ser importadas y analizadas mediante consultas en lenguaje SQL con el fin de realizar búsquedas que permitan obtener o detectar incidentes en las bases de datos o situaciones en las cuales se pueda determinar que la información de los archivos no es consistente porque permite registros dobles que presuntamente han sido alterados en uno de los caracteres que compone su información para permitir la inclusión de un registro diferente.

En síntesis, la información se puede clasificar en:

- Archivos de cuentas o que contienen información contable y requieren de un análisis matemático, financiero y contable.
- Archivos que corresponden a listados de contratos, informes de contratación, o relación de información, que requiere de análisis estadísticos, cantidades y porcentajes.
- Archivos que requieren de un análisis de datos y consultas de tipo SQL para descubrir inconsistencias de información.

9.4. DEFINICIÓN DE HERRAMIENTAS PARA ANÁLISIS DE INFORMACIÓN DIGITAL

La información recibida, de acuerdo con las solicitudes realizadas por cada uno de los integrantes del equipo auditor y conforme a los procedimientos de auditoría establecidos para cumplir cada uno de los objetivos planteados en la asignación realizada, requiere de un tratamiento especial.

Como se definió en el punto anterior, la información recibida se clasifica en tres tipos diferentes: información que requiere la realización de operaciones aritméticas o cálculos contables y financieros, la información que necesita de análisis de cantidades, estadísticas o porcentajes de participación y la información sobre la cual se realizan operaciones de búsqueda de datos, comparación de información u otras operaciones mediante instrucciones SQL o consultas a bases de datos.

Teniendo en cuenta esta clasificación, se ha definido tres (3) herramientas de software principales, dos de las cuales corresponden a software comercial y para el cual la Contraloría General de la república posee la correspondiente licencia (Microsoft Excel e IDEA) y un DBMS gratuito (Microsoft SQL Server Express). Por los volúmenes de información recibidos habitualmente, estas herramientas permiten realizar eficientemente los análisis lógicos y matemáticos requeridos.

9.4.1. Microsoft Excel. Este producto, como se mencionó anteriormente y como lo indican sus características, corresponde a una hoja de cálculo y permite por tanto la realización de cálculos matemáticos principalmente.

Dentro de la información recibida, aquella que requiere efectuar cálculos matemáticos, operaciones aritméticas o generación de análisis a información contable y financiera necesita de una herramienta como esta que contiene funcionalidades como la utilización de fórmulas pre configuradas para realizar diferentes operaciones o la generación de nuevas fórmulas comerciales, contables o aritméticas que permitan efectuar cálculos para verificar los movimientos contables y el uso de recursos financieros en sus correspondientes proporciones conforme lo estable la normatividad colombiana aplicable para cada entidad auditada de acuerdo al sector económico, político y social al que pertenece.

Adicionalmente, Excel permite mediante fórmulas y funciones estadísticas, generar conteos, estadísticas, filtros y consultas sobre listados y relaciones de información relacionada con contratos u otros listados de los cuales se quiera establecer agrupaciones y porcentajes de participación ante un universo determinado con el fin de establecer la cantidad de elementos de un listado que representa las labores o conjuntos de información que gestiona la entidad auditada, organizados o agrupados por un parámetro de clasificación de sus elementos.

9.4.2. IDEA. De acuerdo con la evaluación realizada mediante pruebas de acceso y ejecución de funciones, se establece que permite la realización de consultas automatizadas y generación de estadísticas y datos de análisis de las bases de datos importadas a partir de archivos planos o de texto recibidos.

Esta herramienta es de utilidad cuando se busca obtener resultados como la búsqueda de registros duplicados, coincidencias entre archivos, búsquedas de referencia mediante uno o varios campos de comparación, entre otros.

La cantidad de información que se obtiene de las diferentes funciones incluidas en este producto ayuda a la realización de análisis necesarios para establecer debilidades, deficiencias o fallas en el manejo de los recursos públicos del estado por parte del ente auditado.

Teniendo en cuenta que mucha información, particularmente del sector social y específicamente salud y educación, se acopia en bases de datos gestionadas por sistemas de información y aplicativos administrados desde un punto central hacia toda la nación, la revisión de su calidad, consistencia e integridad constituye un aspecto importante a la hora de establecer su validez como medio soporte para el giro de recursos públicos a las entidades que atienden la población correspondiente.

Por lo anterior IDEA se selecciona como herramienta oficial de análisis de información en bases de datos toda vez que permite reducir el número de transacciones, trámites y cantidad de tiempo invertida al momento de generar resultados de auditoria para definir la gestión y uso de recursos públicos en Colombia.

9.4.3. Microsoft SQL Server Express. Este DBMS gratuito de la compañía Microsoft es de utilidad en el evento en que el anterior producto (IDEA) no pueda ser utilizado por motivos ajenos o por fallas en el token tales como desactualización de su información de acceso o de licencia de uso.

Esta herramienta, en forma similar al software IDEA, permite realizar consultas de información para validar integridad y consistencia de bases de datos, pero con la diferencia de que se requiere conocimientos del lenguaje SQL para diseñar las consultas o queries correspondientes al resultado deseado.

SQL Server Express puede ser utilizado únicamente por personal capacitado y con conocimientos en administración de bases de datos y que cuenten con experiencia en la creación y ejecución de consultas basadas en instrucciones SQL.

Como se menciona anteriormente, se selecciona esta herramienta como respaldo ante situaciones que impidan el uso del software IDEA y, aunque no es tan ágil en términos de tiempo y transacciones como IDEA, permite realizar gran cantidad de consultas a los archivos digitales en formato de texto, garantizando resultados confiables y precisos con respecto a las consultas realizadas.

Estas 3 herramientas seleccionadas se aplican en los diferentes tipos de análisis definidos anteriormente, de acuerdo con lo presentado en la siguiente tabla:

Tabla 4. Herramientas de análisis según información

Tipo de información	Herramienta a utilizar
Relaciones de Contratos reportadas por aplicaciones de software	Microsoft Excel
Información Contractual, reportada por sistemas de información	Microsoft Excel

Fuente: Análisis realizado por el autor del proyecto

Tabla 4. (Continuación)

Tipo de Información	Herramienta a utilizar
Información contable, cuentas por pagar, cuentas por cobrar, balances, informes generados por los sistemas contables implementados.	Microsoft Excel
Cuentas, Balances, Presupuestos, reportes del software contable o aplicaciones utilizadas para el registro contable y financiero.	Microsoft Excel
Registros de afiliados y beneficiarios de los planes de promoción y prevención	Microsoft Excel IDEA IDEA MS SQL Server
Red de prestadores de la EPS. Reportes de afiliados.	IDEA MS SQL Server Microsoft Excel
Reportes generados en archivos planos de afiliados en las vigencias a auditar, reportes de recobros solicitados a FOSYGA de las tecnologías en salud no incluidas en el POS, Base de Datos Única de Afiliados de la EPS.	IDEA MS SQL Server

Fuente: Análisis realizado por el autor del proyecto

9.5. RESULTADOS

Una vez realizados los análisis con base en los requerimientos establecidos por los auditores y sus necesidades de información y de análisis para cumplir con los objetivos propuestos en la asignación de auditoría, se determina a continuación las herramientas que serán utilizadas para examinar la información recibida en medios digitales, así como los métodos y pasos para su adecuado manejo y presentación de resultados.

9.5.1. Definición del tipo de análisis a realizar. En esta primera fase de análisis, se determina el tipo de examen a realizar con base en la información recibida.

9.5.1.1. *Archivos que contienen información contable y requieren de análisis matemático, financiero y contable.* Corresponde a toda la información que la entidad auditada presente y que se relaciona con sus departamentos contables y financieros.

En esta clasificación se encuentra las relaciones de cuentas, facturación, balances, presupuestos, información de gastos y toda la información que refleje la contabilidad de la entidad y la gestión de los recursos financieros que le fueron asignados de acuerdo con el presupuesto nacional.

9.5.1.2. *Archivos que corresponden a listados y requieren de análisis estadísticos, cantidades y porcentajes.* Se refiere a toda la información que se

entrega en listados y que requiere ser organizada, realizar conteos por grupos conformados por un criterio determinado, relaciones de datos que requieren filtros.

En esta clasificación se encuentran los listados de información contractual, listados de elementos, listados de sedes, listados de personas, relación de contrataos para ser clasificadas por tipo de contratación, etc., en fin, toda información que deba ser agrupada, clasificada y se necesite generar estadísticas, porcentajes para estudiar comportamientos en las gestiones.

9.5.1.3. *Archivos que corresponden a registros de información y requieren de un análisis de datos y consultas de tipo SQL.* Son todos aquellos archivos de registros de bases de datos o reportes en archivos planos generados por sistemas de información y/o aplicaciones de software de registro de información.

Aquí se clasifican reportes en archivo plano de sistemas de sectores salud, educación, defensa, etc., tales como Bases de datos de afiliados a sistemas de salud (contributivo y subsidiado), Bases de datos de sistemas de matrículas de instituciones y Ministerio de Educación Nacional, Bases de Datos de registro de procesos judiciales, etc. Se relaciona a toda información que requiera ser validada con respecto a su integridad, consistencia, validez de los datos almacenados de acuerdo con la información adicional registrada.

9.5.2. Solicitud de análisis a realizar. Una vez identificado el tipo de análisis requerido, Se identifica la herramienta de software adecuada.

9.5.2.1. *Archivos que contienen información contable y requieren de análisis matemático, financiero y contable.* Para este tipo de archivos, la herramienta que se adecúa a las necesidades específicas de análisis es Microsoft Excel.

Esta herramienta puede ser utilizada por la mayoría de funcionarios.

9.5.2.2. *Archivos que corresponden a listados y requieren de análisis estadísticos, cantidades y porcentajes.* A este tipo de información se aplica la herramienta Microsoft Excel y las funcionalidades incluidas en él, correspondientes al uso de funciones o creación de fórmulas que generen los resultados requeridos.

El uso de la herramienta, para este tipo de análisis, necesita de un funcionario con conocimientos de Excel, nivel avanzado. En caso de ser necesario debe requerirse el apoyo de un profesional con el conocimiento requerido.

9.5.2.3. *Archivos que corresponden a registros de información y requieren de un análisis de datos y consultas de tipo SQL.* Estos archivos necesitan de la realización de consultas por medio de creación de queries en el lenguaje SQL, por lo cual se utiliza el software IDEA. En caso de no disponer del software instalado

en el computador o no contar con el token correspondiente y configurado, se debe usar Microsoft SQL Server Express.

Es necesario el uso de la herramienta por parte de un funcionario con conocimientos en manejo de bases de datos, lenguaje SQL e importación de archivos planos. El perfil requerido corresponde a un ingeniero de sistemas o un tecnólogo en sistemas.

9.5.3. Procedimiento para el análisis requerido.

Una vez determinada la herramienta, es necesario establecer el procedimiento a seguir con el fin de garantizar un análisis correcto que nos ayude a obtener resultados confiables dentro del proceso auditor adelantado. Lo anterior con el fin de que dichos resultados sean consistentes con la situación examinada y tengan el peso jurídico requerido.

Independientemente del tipo de análisis y la herramienta a utilizar, se debe solicitar al líder de auditoría, el medio de almacenamiento que contiene el archivo electrónico o digital recibido y el cual será objeto del análisis. El funcionario analista de la evidencia procederá a realizar una copia del archivo o archivos que se examinarán en un disco duro interno o externo, o en un dispositivo de almacenamiento USB. Una vez realizada la copia, se debe devolver el medio de almacenamiento con los archivos originales al líder para su almacenamiento temporal durante el desarrollo de la auditoría.

Si los archivos digitales que contienen la información objeto de análisis se encuentran en el archivo de evidencia digital establecido, se debe realizar solicitud a dicha área para que se suministre los medios de almacenamiento para realizar una copia en un medio de almacenamiento diferente (los medios establecidos para la información que se encuentra en auditoría) y posteriormente devolver a dicho archivo en el tiempo establecido.

Los procedimientos de análisis que se deben ejecutar, de acuerdo con el tipo de análisis y la herramienta requerida, son:

9.5.3.1. *Archivos que contienen información contable y requieren de análisis matemático, financiero y contable con Microsoft Excel.* El primer paso a verificar es que el archivo recibido se encuentre en un formato compatible con Microsoft Excel (una hoja de cálculo de Excel, archivo plano, archivo de texto, otros orígenes permitidos).

En primera instancia debemos ejecutar el software y proceder a abrir el archivo recibido. Si el archivo recibido es una hoja de cálculo de Excel, se procede a abrir dicho archivo mediante la opción abrir de la herramienta. Si el archivo pertenece a

otro formato diferente, se debe importar mediante el asistente encontrado en la opción Datos del menú de Microsoft Excel.

El analista del archivo o archivos recibidos, procede a establecer los cálculos que se requieren ejecutar para obtener los resultados esperados.

Determinadas las operaciones necesarias, se extrae las columnas que tienen los datos requeridos a un archivo nuevo, para evitar manipular el archivo fuente y modificar sus datos; luego se inserta una o varias columnas nuevas para incluir las fórmulas que el analista considere para obtener los resultados. Es posible seleccionar fórmulas ya diseñadas, si las mismas se ajustan a los requerimientos de análisis de la auditoría.

9.5.3.2. *Archivos que corresponden a listados y requieren de análisis estadísticos, cantidades y porcentajes.* De igual forma que el ítem anterior, se debe realizar como primer paso, la apertura o la importación del archivo recibido, dependiendo del formato en que se encuentre.

Acto seguido, al igual que el punto anterior, se extrae las columnas que tienen los datos requeridos a un archivo nuevo, para evitar manipular el archivo fuente y modificar sus datos; luego se procede a insertar una columna en la hoja de cálculo para insertar o crear la fórmula que, de acuerdo con el objetivo planteado y los resultados esperados, permitirá realizar el análisis de manera objetiva y puntual, siempre apoyada en los criterios o normas que establecen el cómo se debe gestionar los recursos en cada entidad.

9.5.3.3. *Archivos que corresponden a registros de información y requieren de un análisis de datos y consultas de tipo SQL.* Para este caso, la herramienta de software IDEA, cuenta con un asistente de importación en el cual se puede seleccionar el formato en el cual se encuentra grabado o digitalizado el archivo recibido como evidencia solicitada.

El analista, que en este caso es un funcionario con perfil y conocimientos en sistemas de información y bases de datos, procede a examinar los campos contenidos en el archivo, y la organización y delimitación de campos del mismo.

Una vez determinados los campos, se ejecuta la consulta o las consultas que sean necesarias conforme al objetivo de auditoría o los lineamientos establecidos por el equipo auditor de acuerdo con el procedimiento diseñado y desarrollado.

En caso de requerir confrontación de información con otra fuente o la comparación con otro archivo, dicha fuente o archivo adicional debe ser requerido por el líder de la auditoría en los términos y con las condiciones establecidas en el punto de recolección de evidencia digital.

En este punto es importante aclarar que sí, el funcionario analista no pertenece al equipo auditor, la solicitud de análisis debe ser presentada al Supervisor de Auditoría y/o el Ejecutivo de Auditoría, estableciendo el tipo de información recibida, los objetivos planteados, los resultados esperados y los tiempos establecidos para presentar el examen ejecutado. Este requerimiento debe realizarse mediante un escrito conforme a los lineamientos establecidos en la Gerencia Departamental para la elaboración y envío de comunicaciones oficiales internas, el cual debe contemplar como mínimo:

- Relación de la información a ser analizada.
- Objetivos planteados o requerimientos del análisis.

9.5.4. Presentación de resultados obtenidos.

Una vez los análisis han sido llevados a cabo en su totalidad, el funcionario encargado de realizar dicho examen debe diligenciar el *Reporte de presentación de resultados de análisis de evidencia digital,* especificado en el anexo C del presente documento.

Este documento debe diligenciarse en su totalidad. En caso de que el análisis sea realizado por un funcionario miembro del equipo auditor, el campo correspondiente al oficio de solicitud del análisis debe diligenciarse con la frase: “No aplica, funcionario analista es miembro del equipo auditor”.

Si el análisis fue ejecutado por un profesional que no forma parte del equipo que adelanta el proceso auditor, dicho reporte debe remitirse al líder del equipo auditor, o al supervisor de auditoría mediante comunicación oficial diligenciada y registrada de acuerdo con el procedimiento establecido por la Contraloría General de la República para el envío de comunicaciones oficiales internas.

10. PRUEBA PILOTO

Teniendo en cuenta que se desea contar con una herramienta que ayude a garantizar que un soporte probatorio basado en evidencia digital preste el mérito necesario y suficiente para garantizar su idoneidad y validez dentro de un informe de auditoría y posteriormente dentro de un proceso de responsabilidad fiscal, se realiza una prueba piloto en campo para medir la eficiencia y efectividad de los pasos y controles establecidos en el presente proyecto como base para la construcción del procedimiento correspondiente.

La información recopilada como resultado de cada una de las actividades planteadas dentro del desarrollo metodológico, es desarrollada en las diferentes etapas del proceso con el fin de medir su operación y efectividad como procedimiento adicional a los procedimientos de auditoría planteados por el equipo auditor.

10.1. RECOLECCIÓN DE EVIDENCIA DIGITAL

Se toma como base la información correspondiente a la solicitud de información realizada por los miembros del equipo auditor como base para la ejecución de las pruebas conducentes a determinar cómo se ha usado los recursos públicos entregados por el estado en la entidad vigilada.

Cada una de las solicitudes de información, que requiere información en archivos electrónicos o digitales, es enviada a la entidad haciendo claridad de que cada uno de los archivos que se entreguen debe venir referenciado con los siguientes datos:

- Nombre completo del archivo con la extensión.
- Tamaño en bytes que el archivo ocupa en el medio de almacenamiento entregado
- Fecha y hora de creación del archivo.
- Código HASH calculado con algoritmo MD5.

Las respuestas de los requerimientos de la Entidad, fueron evaluadas por el líder quien es el enlace directo entre el equipo auditor y la entidad auditada y, por tanto, es quien firma las solicitudes de información y recibe las respuestas a las mismas.

La información fue archivada en sus respectivos empaques, como los entrega la entidad, en un espacio diferente al habitual para evitar su manipulación o cualquier situación que pusiera en riesgo su integridad física y lógica.

Se detectó mediante el seguimiento a la prueba realizada que algunos de los medios de almacenamiento no fueron almacenados en un lugar separado de la documentación y que los mismos se encontraban sin ningún tipo de empaque que los protegiera. Durante esta evaluación se encontró que se había recibido diez (10) medios de almacenamiento, entre CD y DVD, de los cuales dos (2) no se encontraban embalados adecuadamente y eran usados eventualmente por los funcionarios. Los dos casos evidenciados fueron revisados y se encontró que la información digital contenida en ellos aún era legible en los computadores, sin embargo, se notó la existencia de pequeños rayones en la superficie donde se graba la información lo que a futuro puede impedir su lectura.

Se evidenció la identificación de los medios de almacenamiento mediante rotulación de la información requerida en la cara del CD o DVD recibido, permitiendo su fácil y rápida identificación, así como un control en cuanto al cumplimiento por parte de la entidad vigilada de cada uno de los requerimientos del grupo auditor.

En conclusión, en esta fase se evidencia que las medidas adoptadas permitieron establecer una forma de identificar la información recibida y controlar los incumplimientos por parte de la entidad auditada. Adicionalmente, un inadecuado manejo y almacenamiento de la información digital recibida, puede ocasionar pérdida de datos, así como el deterioro del material probatorio que soporta un hallazgo con presunta incidencia fiscal.

10.2. ALMACENAMIENTO DE EVIDENCIA DIGITAL

Teniendo en cuenta que es la primera vez que se realiza este procedimiento en una auditoría y que el mismo aún no ha sido implementado en la Gerencia Departamental, no es posible realizar las pruebas correspondientes al archivo de las evidencias, registro y custodia que garantice su conservación.

Solo fue posible medir el nivel de conservación de los medios digitales durante el proceso auditor. En este aspecto se evidencia que la inadecuada disposición de los medios de almacenamiento pone en riesgo la integridad y disponibilidad de la información digital recibida.

Adicionalmente, la auditoría definida para la obtención de información y realización de la prueba piloto, a la fecha se encuentra en etapa de ejecución y no se ha obtenido la totalidad de información en medios de almacenamiento para su archivo en un espacio de la Gerencia Departamental.

Una vez se presente a consideración de los directivos el procedimiento y la socialización de la importancia de su implementación y los beneficios que trae a los procesos auditores y posteriores labores, se definirá la realización de otra prueba

complementaria que establezca los parámetros finales de puesta en marcha de dicho procedimiento.

10.3. ANALISIS DE INFORMACIÓN EN EVIDENCIA DIGITAL

Durante la auditoría se recibió información digital que contiene tanto información contable como relaciones de contratos, de usuarios afiliados a salud, de Instituciones prestadoras de salud y bases de datos de diferentes fuentes.

Previo al uso de la información almacenada en los medios ópticos recibidos, se realiza la verificación de cada uno de los códigos HASH y datos identificadores (nombre, fecha de creación y tamaño en bytes) de los archivos contenidos en dichos medios con el fin de confirmar que los mismos correspondan a los especificados en los oficios o comunicaciones que evidencian la entrega por parte de la entidad que se está auditando.

Para calcular el código hash y consultar los datos identificadores, se hace uso de la herramienta hashmyfiles, la cual permite realizar la consulta correspondiente de todo el medio óptico y además, obtener los otros datos identificadores. Esta herramienta permite calcular el código hash utilizando diferentes algoritmos criptográficos, entre los cuales se encuentra el MD5 que es el solicitado a las entidades.

Una vez verificado que los códigos y demás información identificativa de los archivos concuerdan con la comunicada por la entidad, se procede a realizar el análisis correspondiente dependiendo del tipo de información, tipo de análisis requerido y los objetivos a alcanzar.

La información contable, solicitada por los dos contadores públicos asignados al equipo auditor, fue recibida y analizada por ellos mismos mediante el uso de la herramienta Microsoft Excel, previa copia desde el medio de almacenamiento digital en el momento de la entrega.

Los resultados fueron consignados en un formato de papel de trabajo, diseñado por los auditores de acuerdo con los lineamientos y condiciones establecidas por la Guía de Auditoría de la Contraloría General de la República.

No se cumplió con el diligenciamiento de la información en el formato establecido en el Anexo C, *“Reporte de presentación de resultados de análisis de evidencia digital”.*

Las relaciones de contratos fueron examinadas y filtradas por los dos funcionarios abogados, quienes se encargaron de establecer filtros con el uso de la herramienta

Microsoft Excel para determinar cantidades de contratos por modalidad de contratación, estadísticas por proveedores, contratistas y por montos, entre otros.

De igual forma no se presenta formato de reporte diligenciado (Anexo C). Los resultados y el procedimiento en general se diligencian en el papel de trabajo diseñado por los auditores con perfil abogado.

Por último, la información relacionada con las bases de datos, se recibe y realiza copia en dispositivo pendrive USB por parte del Ingeniero de Sistemas asignado al equipo auditor, quien se encarga de realizar consultas, mediante el uso de la herramienta Microsoft SQL Server Express, ya que se encuentra fuera de la Gerencia Departamental y no cuenta con el software IDEA a su disposición en el equipo de cómputo asignado.

Se realiza consultas de información para determinar, de la base de datos de recobros, cuántos fueron radicados en 2014 y cuántos en el año 2015, además se consulta la cantidad de recobros sustentados en tutelas y comités técnicos científicos.

Dentro del desarrollo del procedimiento, se realiza cruces de información (consultas mediante sentencias SQL para realizar comparaciones entre dos fuentes) con la información de fallecidos para establecer prestaciones de servicios a usuarios que ya se encontraban muertos.

Los análisis permitieron detectar posibles inconsistencias dentro de las bases de datos evaluadas, conformando un posible hallazgo fiscal.

Es muy importante que de esta actividad se presente el reporte de resultados debidamente diligenciado y que, ya que la auditoría no se ha finalizado, aún se encuentra en su diligenciamiento.

Se observa dilación en tiempo para su diligenciamiento, lo cual puede ocasionar errores al no registrar las acciones realizadas en tiempo real.

Es importante que la información obtenida como soporte en desarrollo de la auditoría, sea almacenada adecuadamente durante y después del proceso auditor, ya que, al detectarse un posible hallazgo fiscal, esta será requerida por los funcionarios que adelanten el respectivo proceso de responsabilidad fiscal que busca resarcir el daño recuperado mediante la recuperación de los recursos fiscales afectados.

En conclusión, se observa que los pasos establecidos pueden ayudar a garantizar que la información se pueda conservar y preste los méritos suficientes como acervo probatorio para demostrar una acción o acciones inadecuadas u omitidas por parte de la entidad auditada que llevaron a la ocurrencia de un hecho que ocasionó un

daño fiscal y que, fue detectado por el equipo auditor de manera correcta y completa.

11. PROCEDIMIENTO FINAL

Una vez acopiados los resultados de cada etapa, y verificados mediante la realización de una prueba piloto, se procede a acopiar toda la información con el fin de elaborar el manual del procedimiento que será presentado a los directivos correspondientes para que sea evaluado y, en caso de ser aceptado, implementado en el área de control fiscal micro de la gerencia departamental.

El manual del procedimiento se diseña y elabora teniendo en cuenta los siguientes componentes:

- Portada
- Introducción
- Objetivos
- Marco Legal y Conceptual
- Ámbito de Aplicación
- Alcance
- Políticas Generales
- Descripción del Proceso
- Responsables
- Referencias
- Glosario.

El manual con su diseño preliminar, incorporando cada uno de los resultados obtenidos en el presente proyecto, así como los componentes mencionados se presenta como anexo al final del presente documento, identificado como “MANUAL DE PROCEDIMIENTOS - RECOLECCION, CADENA DE CUSTODIA Y USO DE EVIDENCIA DIGITAL DENTRO DEL DESARROLLO DE PRUEBAS DE AUDITORÍA EN LA GEERENCIA DEPARTAMENTAL COLEGIADA VALLE DEL CAUCA DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA” (Anexo E).

12. RESULTADOS E IMPACTO

El presente trabajo de grado se realizó con el propósito de presentar una herramienta que ayude a obtener, de manera correcta y apropiada, evidencia electrónica o digital, buscando que la misma mantenga su integridad, disponibilidad y confidencialidad por medio de una adecuada disposición y conservación.

Con este trabajo se busca alcanzar los siguientes resultados e impacto:

12.1. RESULTADOS

La finalidad del presente trabajo es la generación de un procedimiento que sirva como instrumento para recibir, conservar y realizar los análisis necesarios sobre la información que se recibe como insumo para el desarrollo de las labores de una auditoría gubernamental y las cuales se encuentran almacenadas en medios digitales o electrónicos.

Además de este resultado se identifica cada uno de los procesos que se realizan desde que se solicita la información al ente auditado, hasta su almacenamiento y posterior requerimiento en caso de necesitar la ejecución de posteriores análisis o demostraciones en procesos de responsabilidad fiscal.

12.2. IMPACTO

Con este procedimiento se busca garantizar que la información recibida, mantenga su integridad y, por medio de una adecuada organización, su disponibilidad y confidencialidad.

La información que se reciba, almacene y analice, será un soporte probatorio idóneo para ser presentado como una prueba suficiente y pertinente dentro de un proceso de responsabilidad fiscal iniciado a partir de un hallazgo fiscal presentado por un grupo auditor y que busca resarcir un daño fiscal causado.

El aumento en el nivel de efectividad de un proceso que se sustenta en un hallazgo debidamente configurado y que se apoya en soportes probatorios digitales, redundará en un aumento del nivel de confianza de la ciudadanía y el gobierno en una entidad cuyo objetivo y misión es realizar un control eficiente, efectivo y eficaz sobre el uso de los recursos de la nación y la reducción de tiempo en determinar responsabilidades, daños fiscales, evitando o disminuyendo la realización de pruebas adicionales.

13. DIVULGACION

El Procedimiento diseñado, como producto final del proyecto desarrollado, será presentado a los directivos de la Gerencia Departamental del Valle del Cauca de la Contraloría General de la República para su respectivo análisis e implementación en esta Gerencia como una propuesta de mejoramiento de los procedimientos para la recepción, conservación y uso adecuado de la evidencia digital aportada por los entes auditados.

Si los directivos autorizan su implementación y uso, el mismo será divulgado a cada uno de los funcionarios del grupo de Vigilancia Fiscal de la Gerencia Departamental Colegiada Valle del Cauca como un documento digital en formato PDF que será dispuesto en el servidor de archivos de dicha Gerencia Departamental.

RECOMENDACIONES

- Los procedimientos que se incluyen en el producto final del presente proyecto de grado, deben ser ejecutados exactamente como se redactaron y en el orden que se ha establecido para, de esta manera, salvaguardar la información que se ha recaudado como evidencia digital.

- Es importante que las condiciones de conservación establecidas para los medios de almacenamiento se configuren en concordancia con las recomendaciones de seguridad y protección establecidas por el fabricante de dichos medios, como se establece en el manual, producto del presente proyecto de grado.

- Es conveniente, durante la implementación del manual de procedimientos anexo, efectuar seguimiento del cumplimiento de cada uno de los pasos establecidos para la recolección, conservación y uso de evidencia digital en el proceso auditor, conforme a los mecanismos de evaluación de procedimientos de la Contraloría General de la República, para garantizar su efectividad y correcto funcionamiento.

- Socializar el documento a los diferentes auditores mediante comunicación escrita y capacitaciones, con el fin de interiorizar la necesidad y utilidad de contar con procedimientos que garanticen su autenticidad, confiabilidad, suficiencia y conformidad con las leyes para así, prestar el mérito jurídico y legal necesario para sustentar un hallazgo y el posterior proceso de responsabilidad fiscal que de él se derive.

- Adicionalmente al procedimiento generado, las herramientas informáticas y tecnológicas que se requieren para el desarrollo de los diferentes pasos establecidos en el manual de procedimientos generado, deben contar con un soporte técnico adecuado y periódico que impida que las actividades encaminadas a asegurar la evidencia digital no se cumplan y pongan en riesgo la confidencialidad, integridad y disponibilidad de la evidencia digital recibida y la información contenida en ella.

CONCLUSIONES

- La información recibida en medio digital o electrónico, como soporte de las pruebas de auditoría adelantadas por la Contraloría General de la República, actualmente no cuentan con un procedimiento orientado a garantizar su eficiencia, confiabilidad, pertinencia y validez dentro de un informe de auditoría o un proceso de responsabilidad fiscal.

- Así como existen avances en el registro y proceso de información generada por las entidades objeto de estudio mediante el uso de herramientas de software y sistemas de información, se debe contar con mecanismos apoyados en estas tecnologías que permitan la adecuada obtención de la evidencia digital dentro de un proceso auditor.

- El análisis realizado en el desarrollo del proyecto permite observar que no se cuenta con procedimientos técnicos, soportados en manejo de evidencia digital, que aseguren la procedencia de un documento, así como su validez como prueba dentro de un proceso de responsabilidad fiscal.

- Un conjunto de medidas de conservación establecidas técnicamente, teniendo en cuenta las especificaciones de fábrica para el bodegaje, custodia y manejo de los medios de almacenamiento disminuye los riesgos de afectar la integridad y disponibilidad de la información grabada en ellos.

- La implementación de un procedimiento normalizado para la adquisición, custodia y manejo de evidencia digital brinda garantías en el uso de la misma dentro de un proceso, toda vez que se usan herramientas técnicamente seleccionadas para establecer su idoneidad, validez, pertinencia y suficiencia, así como su integridad, confidencialidad y disponibilidad.

BIBLIOGRAFIA

ARELLANO, L. y CASTAÑEDA C. La cadena de custodia informático-forense. En: Revista ACTIVA. Enero-junio 2012. no. 3, p. 67-81.

CALAMEO. Guía para el manejo de evidencia digital [En línea]. <http://es.calameo.com/read/004053479c7bcc08c68de> [citado en 26 de octubre de 2015]

CANO, J. Introducción a la informática forense. En: Sistemas. no. 96, p. 64-73.

CANO MARTINEZ, Jeimy J. Computación forense. Descubriendo los rasgos informáticos. México, D.F.: Alfaomega, 2009. 344p. ISBN 978-958-682-767-6.

CONTRALORIA GENERAL DE LA REPUBLICA. ¿Qué es la Contraloría? [En línea]. <http://www.contraloria.gov.co/web/guest/que-es-la-cgr> [citado en 27 de septiembre de 2015]

EL BLOG DEL PERITO INFORMATICO. La cadena de custodia aplicada a la informática - I [En línea]. <http://www.informaticoforense.eu/la-cadena-de-custodia-aplicada-a-la-informatica-i> [citado en 5 de diciembre de 2017]

ESCORCIA OYOLA, O. MANUAL PARA LA INVESTIGACIÓN Guía para la formulación, desarrollo y divulgación de proyectos. Bogotá. 2010.

EXPLORABLE. Definición de un problema de investigación. [En línea]. https://explorable.com/es/definicion-de-un-problema-de-investigacion [citado en 18 de julio de 2016]

GAVIRIA, PABLO ANDRÉS. Propuesta de un modelo de procedimiento para el tratamiento de la evidencia digital, acorde a la normatividad colombiana sobre delitos informáticos. Monografía. [En línea]. <http://repository.unad.edu.co/handle/10596/4008> [Ingeniero de Sistemas] Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas e Ingenierías [citado en Octubre de 2016]

MARQUÉS-ARPA, T., y SERRA-RUIZ, J. Cadena de Custodia en el Análisis Forense. Implementación de un Marco de Gestión de la Evidencia Digital. Septiembre de 2014. Alicante.

MINISTERIO DE DEFENSA. Soporte legal de la evidencia digital en un incidente informático. [En línea]. <http://www.colcert.gov.co/sites/default/files/evidencia_digital.pdf> [citado en 24 de octubre de 2015]

SUAREZ SIERRA, L., MEJÍA ÁLVAREZ, D., VILLERO MAESTRE, F., HERRERA MORALES, E., y DÍAZ PLATA, N. GUIA PROPUESTA DE PROYECTO DE INVESTIGACION. UNIVERSIDAD POPULAR DEL CESAR. 2011.

TODO ES ELECTRÓNICO. ISO 27037 Directrices de gestión de evidencias electrónicas. [En línea]. <http://inza.wordpress.com/2013/06/11/iso-27037-directrices-de-gestion-de-evidencias-electronicas> [citado en 28 de septiembre de 2015]

ANEXOS

Anexo A. Formato de Entrevista aplicado a los profesionales que componen el equipo auditor

PROYECTO DE GRADO ***ESPECIALIZACION EN SEGURIDAD INFORMÁTICA***	
FORMATO DE ENTREVISTA	
FECHA:	
NOMBRE:	
PROFESION:	
CARGO:	

1. Relacione a continuación la información requerida en los procedimientos de auditoría que realiza

2. ¿Cuál de los anteriores ítems requieren ser entregados por el ente auditado en un medio digital?

3. ¿Cómo se realiza la solicitud de información en medio digital al ente auditado?

4. ¿Qué operaciones requiere realizar con la información recibida en medios digitales?

5. ¿Utiliza programas y/o aplicaciones de software para analizar la información recibida? En caso de que la respuesta sea afirmativa, especifique cuáles utiliza.

6. ¿La información que la entidad auditada suministra en medios digitales, permite ser analizada sin inconvenientes? En caso de presentarse inconvenientes, relacione los más comunes.

7. ¿Ha requerido solicitar apoyo de profesionales con experticia en el manejo y análisis de información suministrada en medios digitales para su estudio y generación de consultas? En caso de ser afirmativa la respuesta, enumere las principales razones para hacerlo.

8. ¿Cuáles son los medios que la entidad auditada utiliza para suministrar la información digital solicitada?

9. ¿La información suministrada por la entidad en medios como CD, DVD, USB, está rotulada de manera que permita su fácil identificación? En caso de que

la respuesta no sea afirmativa, ¿Cuál cree usted que es la manera más adecuada de identificar un medio de almacenamiento?

10. ¿Al suministrar información digital (archivos electrónicos, CD, DVD, USB, adjuntos en correos electrónicos), la entidad certifica de alguna manera que la información corresponde a reportes generados por programas, aplicaciones o sistemas de información institucionales? En caso de que la respuesta sea afirmativa, ¿qué características se relacionan como parámetros para garantizar su autenticidad con respecto a la fuente?

11. En caso de que la entidad suministre copia de sus archivos digitales o electrónicos, en respuesta a un requerimiento del grupo auditor, ¿cómo se valida su confiabilidad y autenticidad?

12. Una vez la información se recibe en un medio físico de almacenamiento (CD, DVD, USB), ¿cómo es archivada para su posterior localización y consulta?

13. ¿Los análisis o pruebas de auditoría realizados sobre la información suministrada por el ente auditado se ejecutan directamente sobre los archivos digitales recibidos? En caso de responder afirmativamente, especifique los pasos más comunes que realiza.

Anexo B. Inventario de Información o Evidencia Digital recibida

Espacio para Logo Institucional	CONTRALORÍA GENERAL DE LA REPÚBLICA Gerencia Departamental Colegiada Valle del Cauca
Inventario de información o evidencia digital recibida durante el proceso auditor	
Entidad Auditada:	
Asunto a auditar:	
Vigencia:	
Equipo auditor:	

Referencia	Medio de Almacenamiento	Cantidad de archivos	Fecha de Recepción	Observaciones
Acorde con la Guía de Auditoría para las comunicaciones oficiales	CD. DVD. Dispositivo extraíble USB. Correo Electrónico.	Número entero que identifique la cantidad de archivos contenida en el medio entregado	Fecha y hora en que se recibe la información	Situaciones o características que sirven como identificación especial del medio recibido

Anexo C. Reporte de presentación de resultados de análisis de evidencia digital

Contraloría General de la República	
Gerencia Departamental Colegiada Valle del Cauca	
FORMATO DE PRESENTACIÓN DE RESULTADOS DE ANÁLISIS DE EVIDENCIA DIGITAL	
Auditoría que requiere el análisis:	Nombre o descripción de la auditoría que requiere del análisis.
Auditor que solicita el análisis:	Funcionario solicitante del análisis.
Oficio de solicitud de análisis:	Número y fecha de la solicitud del análisis.
Auditor que realiza análisis:	Auditor que realiza análisis de la evidencia.
Fecha realización de análisis:	Fecha en que se finaliza el análisis solicitado.

1. Información Recibida como Evidencia Digital a Analizar:
Relación detallada de la información digital fuente para ser analizada. Incluya Nombre de archivo, fecha de creación, código de almacenamiento, código Hash (MD5).

2. Objetivos planteados para el análisis de la evidencia:
Relacione cada uno de los objetivos planteados en la solicitud de análisis realizada.

3. Herramienta seleccionada para realizar el análisis correspondiente:
Registre Nombre y versión del software o productos de software utilizados para el análisis.

4. Descripción del Procedimiento Realizado:
Describa detalladamente los pasos realizados durante el análisis, describiendo la información, modificaciones y pasos del procedimiento

5. Resultados Obtenidos con el procedimiento:
Describa los resultados obtenidos en cada uno de los análisis realizados.

6. Relación de archivos anexos al presente reporte:
Relacione los archivos que contienen los resultados del análisis realizado y que deben consignarse anexos al presente reporte

7. Observaciones.
Registre en este espacio las observaciones que deban tenerse en cuenta por parte del funcionario que solicita y requiere de los resultados del análisis.

8. Firma Funcionario analista.
Digite Nombre, Profesión y Cargo del funcionario que realiza el análisis. Firma del funcionario relacionado.

Anexo D. RESUMEN ANÁLITICO RAE

Título de Documento	Diseño e implementación de un procedimiento para la recolección, cadena de custodia y uso de evidencia digital dentro del desarrollo de pruebas de auditoría en la Gerencia Departamental Valle del Cauca de la Contraloría General de la República
Autor	ARTEAGA G, Yeimy Andrés
Palabras Claves	Evidencia digital, pruebas de auditoría, cadena de custodia, ISO 27037, integridad, suficiencia, pertinencia, medios de almacenamiento.

Descripción

El presente documento es un proyecto aplicado que se desarrolla con el objetivo de presentar un procedimiento normalizado para la recolección, custodia y manejo de información recibida, en medio digital o electrónico, como soporte de pruebas realizadas en el desarrollo de auditorías gubernamentales efectuadas por la Gerencia Departamental Valle del Cauca de la Contraloría General de la República para de esta manera garantizar la confiabilidad, integridad y disponibilidad de la evidencia digital recaudada dentro de un proceso de responsabilidad fiscal.

Fuentes Bibliográficas	- Mosquera González, J. A., Certain Jaramillo, A. F., & Cano, J. J. (2005). Evidencia Digital: contexto, situación e implicaciones nacionales. Revista De Derecho Comunicaciones Y Nuevas Tecnologías, 175-205. - Plazas, A. R., & Cano, J. J. (2006). Valoración de la evidencia digital: Análisis y propuesta en el contexto de la administración de justicia en Colombia. Revista De Derecho Comunicaciones Y Nuevas Tecnologías, 95-121. - Cano Martínez, J. J. (2010). El peritaje informático y la evidencia digital en Colombia: conceptos, retos y propuestas / Jeimy José Cano Martínez, (coordinador); GECTI. Bogotá: Universidad de Los Andes, Facultad de Derecho, 2010. - Valencia Duque, Francisco Javier (2012) El e-control, estado actual y perspectivas en el

	control fiscal colombiano. Seminarios Control en Línea, noviembre 15 de 2012; noviembre 30 de 2012 y diciembre 12 de 2012, Bogotá, Cartagena y Cali (Colombia). - Bogotá, P. D., & Claudia, M. P. Evidencia Digital en Colombia: Una reflexión en la práctica, publicado en Revista de Derecho Informático Alfa-redi núm. 107 de junio de 2007. - Fiscalía General de la Nación (2004). Manual de procedimientos del sistema de Cadena de Custodia. Bogotá, DC.

Contenido:

El presente proyecto, tiene como sujeto de aplicación a la Contraloría General de la República quien es el máximo órgano de control del Estado y se encarga de la vigilancia sobre los recursos de la Nación, examinando si estos son utilizados de acuerdo con la normatividad existente y las políticas públicas establecidas, mediante la planeación y ejecución de auditorías gubernamentales.

La ejecución del proyecto centra su análisis en la adquisición, custodia y el manejo de toda la evidencia digital que se recauda por parte de los grupos auditores de la Contraloría General de la República.

Este documento tiene como finalidad principal ser una guía para la adecuada utilización y disposición de la información electrónica, para que pueda ser usada como un soporte válido dentro de un proceso auditor y como material probatorio en un proceso de responsabilidad fiscal que busca resarcir el daño causado por un uso indebido de los recursos públicos de la Nación.

Los soportes obtenidos mediante la realización de pruebas de auditoría, y los cuales se encuentran en archivos digitales, electrónicos y/o bases de datos, deben contar con los requerimientos necesarios e idóneos para ser tenidos en cuenta como acervo probatorio dentro de un proceso de Responsabilidad Fiscal que pueda surgir del ejercicio auditor; sin embargo, actualmente los medios, mecanismos, procedimientos e instrumentos con los que la Gerencia Departamental del Valle del Cauca cuenta para realizar esta labor, no garantizan totalmente la eficiencia requerida en el desarrollo de labores de obtención de evidencia digital que permita asegurar que dicha evidencia cumpla con los requisitos para ser tenida en cuenta como ilustración suficiente de la situación observada.

Al no contar con herramientas o procedimientos claramente definidos para el

manejo de este tipo de evidencia, no se puede asegurar su integridad y confiabilidad tanto a nivel de los datos que la componen como el medio físico que la almacena.

Un proceso de Responsabilidad Fiscal se genera cuando en una auditoría se obtienen pruebas de un indebido uso de los recursos de la Nación, el cual como consecuencia deriva en un daño fiscal. Una situación de estas, detectada en el ejercicio auditor, se informa como hallazgo fiscal y posteriormente se comunica a un grupo especializado que se encarga de realizar el proceso correspondiente con el fin de establecer el daño causado, los responsables y el valor del mismo para de esta forma buscar resarcirlo. Un hallazgo, y posteriormente un proceso de responsabilidad fiscal que se base en una prueba realizada a información almacenada en medios digitales, puede no tener la certeza suficiente o la garantía de que esa información corresponde a la realidad del ente auditado y que la misma, de acuerdo con la normatividad relacionada, fue tomada garantizando que corresponde a información oficial de la entidad. Una prueba que no cumple con estos requisitos ocasiona que un proceso se declare nulo al no cumplir el debido proceso o no garantizar que corresponde a una fuente oficial y se haya obtenido correctamente de la fuente.

El proyecto, en aras de corregir las debilidades y situaciones que pueden en un momento impedir un buen recaudo de pruebas que soporten las situaciones evidenciadas en el proceso auditor, tiene como objetivo general: implementar un procedimiento de recolección, cadena de custodia y uso de evidencia digital que permita garantizar la idoneidad y validez de dicha evidencia, obtenida dentro de una auditoría gubernamental como prueba suficiente, confiable y pertinente en la Gerencia Departamental Valle Del Cauca de la Contraloría General de la Republica.

Para el desarrollo y cumplimiento de este objetivo se establece un plan de trabajo basado en el cumplimiento de los siguientes objetivos:

- Definir los tipos de información y medios idóneos que se deben utilizar para la recolección de evidencia digital.

- Establecer los pasos, medios y responsables para el manejo y control de la evidencia digital recaudada en las auditorías.

- Formalizar las herramientas de software idóneas para el análisis y uso de la evidencia digital, orientadas a obtener resultados claros, confiables y que revelen la realidad de lo observado.

- Verificar, mediante una prueba piloto, la efectividad y eficiencia de los procedimientos, herramientas y pasos establecidos para garantizar la validez e

idoneidad de la evidencia digital recaudada.

- Diseñar un procedimiento para la recolección, cadena de custodia y uso de la evidencia digital obtenida a partir de la práctica de pruebas de auditoría.

Con la aplicación de la metodología seleccionada, se recopila la información necesaria en cada una de las fases, determinando así una serie de requerimientos, pasos, responsables y requisitos necesarios para su aplicación en lo relacionado con el manejo de la evidencia digital dentro de los procesos de auditoría gubernamental.

Se toma como base el desarrollo de los procedimientos llevados a cabo por un grupo auditor interdisciplinario con el fin de establecer métodos, mecanismos y procedimientos actuales para ser evaluados técnicamente y así identificar situaciones en las cuáles se requiera aplicar controles adicionales para proteger y salvaguardar la información electrónica o digital recaudada.

El análisis realizado tiene como fundamento principal la normatividad colombiana sobre control fiscal y algunos aspectos del estándar ISO/IEC 27037:2012 en lo relacionado con la cadena de custodia, almacenamiento de información y métodos que permitan su análisis sin alterar la prueba obtenida.

En el desarrollo del proyecto se establece la forma como el grupo auditor debe solicitar la información, indicando características de la misma y los medios admitidos con el fin de establecer formalmente su validez y procedencia.

Se define dentro del procedimiento elaborado, los pasos para la identificación, archivo y manejo de los medios de almacenamiento que contienen la información recaudada dentro de los procesos auditores con el fin de reducir el riesgo de pérdida de datos que afectan la integridad y validez de las pruebas dentro de un proceso.

Finalmente, se genera un procedimiento que establece la forma de solicitar información digital o electrónica, los pasos requeridos para garantizar un correcto almacenamiento y cómo realizar las pruebas a la información sin afectar la prueba originalmente obtenida.

Metodología

En el presente proyecto se utilizó un enfoque cuantitativo orientado a medir la eficiencia, integridad, pertinencia y confiabilidad de la información electrónica recibida en medio digital dentro de una auditoría gubernamental en la Contraloría General de la República.

Se adoptó también un enfoque exploratorio, descriptivo y explicativo, ya que este proyecto está orientado al estudio de las fuentes y modelos relacionados con el manejo de evidencia digital para generar un procedimiento formal que adopte la especificación de requisitos y el uso de técnicas y mecanismos que sean aplicables dentro de un proceso de auditoría gubernamental.

Para el desarrollo de los estudios correspondientes, se diseñó y ejecutó un plan de trabajo orientado por 3 etapas:

- Estudio y definición de mecanismos y medios para la recolección de evidencia digital como soporte de pruebas de auditoría.
- Análisis y selección de lugares, medios y pasos para la custodia de los archivos electrónicos y digitales recolectados en una auditoría.
- Selección de herramientas para el manejo y análisis de herramientas para su manejo y análisis.

Finalmente, con los datos e información recolectada, se procedió a validarla, ajustarla y posteriormente generar el documento que contiene el procedimiento diseñado y validado, que será presentado para su aprobación e implementación.

Recomendaciones.

- Se debe cumplir con los procedimientos para solicitar información digital con el fin de contar con soportes que definan de manera inequívoca su origen y validez como datos oficiales de la entidad examinada.
- Es importante acatar las medidas de conservación necesarias, establecidas en las especificaciones de fábrica, para la disposición y manejo de los medios de almacenamiento con el fin de mantener la integridad de los datos almacenados.

Anexo E. MANUAL DE PROCEDIMIENTOS

RECOLECCION, CADENA DE CUSTODIA Y USO DE EVIDENCIA DIGITAL DENTRO DEL DESARROLLO DE PRUEBAS DE AUDITORÍA EN LA GEERENCIA DEPARTAMENTAL COLEGIADA VALLE DEL CAUCA DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA

SANTIAGO DE CALI
2017

TABLA DE CONTENIDO

Pág.

INTRODUCCIÓN

En un mundo en el que las tecnologías de la información han volcado la generación y uso de información a los medios de almacenamiento digitales, se hace necesario tomar medidas que permitan su adquisición, conservación y manipulación, de tal manera que no se ponga en riesgo ni se comprometa su integridad, confidencialidad y disponibilidad.

Dentro de las pruebas que se realizan, en desarrollo de una auditoría o actuación especial a una entidad vigilada, por parte de la Contraloría General de la República, se debe solicitar y analizar información que se encuentra almacenada en dispositivos electrónicos o digitales y, por tanto, con el fin de asegurar su integridad y su autenticidad con respecto a la fuente que lo genera, es necesario observar prácticas que garanticen que dicha información no será modificada y será conservada manteniendo las mismas características que contenía cuando la entidad hizo la entrega.

Un adecuado procedimiento que permita recibir, conservar y analizar información electrónica o digital, manteniendo su integridad principalmente, nos ayuda a garantizar pruebas y resultados de auditoría confiables, suficientes y relevantes dentro de la situación que se pretende demostrar como hallazgo.

Adicionalmente, un hallazgo que depende de evidencia en medios digitales como prueba, y que se encuentre bien sustentado y soportado, permitirá resarcir el daño evidenciado, resultando en un beneficio para los recursos de la Nación y de los colombianos.

OBJETIVOS

- Establecer políticas y lineamientos para el tratamiento de información digital o electrónica dentro de un proceso auditor, que garantice la eficacia y efectividad de dicha información como soporte dentro de un proceso auditor y/o un proceso de responsabilidad fiscal.

- Fortalecer la labor auditora en la Gerencia Departamental Colegiada del valle del Cauca, mediante la formulación de un procedimiento técnico objetivo para la recepción, disposición y uso de información en medios digitales o electrónicos.

- Contar con directrices que ayuden a establecer una metodología de conservación de la información digital recibida o recaudada, que pueda ser usada posteriormente, prestando el mismo mérito inicial como material probatorio relevante, suficiente y confiable.

MARCO LEGAL Y CONCEPTUAL

De acuerdo con la ISO/IEC 27037:2012 la evidencia digital es gobernada por tres principios fundamentales: la relevancia, la confiabilidad y la suficiencia. Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital, bien ésta sea utilizada para que sea admisible en una corte o no.

La relevancia trata de la pertinencia de elementos en una situación específica analizada para probar una hipótesis sobre los hechos investigados.

La confiabilidad se refiere a la auditabilidad y repetibilidad de la evidencia recaudada.

La suficiencia indica que la evidencia digital obtenida es suficiente para sustentar los hallazgos y verificar las afirmaciones emitidas sobre la situación examinada y evidenciada.

Ley 1273 del 5 de enero de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Sentencia C-662 de 8 de junio de 2000. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Resolución 0-6394 del 22 de diciembre de 2004. Por medio de la cual se adopta el manual de procedimientos del Sistema de Cadena de Custodia para el Sistema Penal Acusatorio.

Acuerdo PSAA06-3334 del 2 de marzo de 2006. Por el cual se reglamentan la utilización de medios electrónicos e informáticos en el cumplimiento de las funciones de administración de justicia.

ÁMBITO DE APLICACIÓN

El presente procedimiento será aplicado dentro de las auditorías planeadas por Nivel Central y asignadas a la Gerencia Departamental Colegiada del Valle del Cauca, a partir de su aprobación por los directivos correspondientes.

Es responsabilidad de cada grupo auditor asignado, la observancia y cumplimiento de los lineamientos establecidos en el presente manual de procedimientos con el fin de garantizar la confiabilidad de los soportes obtenidos en medios digitales y de los resultados de las pruebas realizadas con los mismos como acervo probatorio de un hallazgo fiscal y un posterior proceso de responsabilidad fiscal.

ALCANCE

El presente manual establece, exclusivamente, los procedimientos y lineamientos para realizar una adecuada recepción, almacenamiento y tratamiento de información recibida en medio digital o electrónico dentro del desarrollo del proceso auditor que la solicita a la entidad vigilada para ser analizada de acuerdo con los objetivos establecidos en la asignación de auditoría realizada.

El almacenamiento hace referencia a la disposición de la información y los medios utilizados por el ente auditado para su entrega durante la ejecución y desarrollo de la auditoría, así como su posterior disposición como archivo de evidencia digital que puede ser usado eventualmente en caso de requerir soportar un proceso de responsabilidad fiscal.

Durante la implementación del procedimiento, es necesario realizar jornadas de capacitación y sensibilización en las ventajas de contar con mecanismos de control que permitan asegurar la eficiencia y confiabilidad de una prueba basada en archivos digitales o electrónicos.

POLÍTICAS GENERALES

La Contraloría General de la República es la encargada de ejecutar las auditorías tendientes a establecer si las entidades o particulares que administran los recursos públicos del orden estatal han hecho un uso eficiente, eficaz y efectivo de los mismos en cumplimiento de los lineamientos y directrices establecidos por las leyes y normas estatales para tal fin.

Dentro de los procesos misionales de la Contraloría General de la Republica se encuentra el de Control Fiscal Micro, que es el encargado de planear y ejecutar las auditorías que se establecen cada año en el Plan Anual de Vigilancia Fiscal (PAVF), previo análisis realizado por la Oficina de Planeación y los directivos de la Contraloría General de la República.

La Contraloría General de la República ha creado una guía de auditoría en la cual se establecen los diferentes procedimientos, pasos y actividades que se deben desarrollar por parte de los diferentes miembros del equipo auditor y los directivos que se encargan de la supervisión y cumplimiento de dichas auditorías. El proceso detallado desde la planeación del PAVF y de la ejecución de las auditorías, así como sus etapas, se encuentras enmarcadas en la guía de auditoría actualizada a abril de 2015. Actualmente se ha establecido la realización de auditorías especiales, para las cuales se ha elaborado guías específicas y que, durante el actual periodo se encuentra en etapa de implementación.

Las etapas y los procedimientos establecidos para el desarrollo de las auditorías no han tenido cambios que afecten el procedimiento que se detalla en el presente manual. Las guías de auditoría que se mencionan y que rigen la realización de los procesos auditores en la Contraloría General de la República se encuentran disponibles en la página web[9] oficial de la entidad.

Toda solicitud de información realizada a la entidad vigilada, debe cumplir los requerimientos establecidos para el envío de comunicaciones oficiales, los cuales se encuentran especificados en los manuales internos de calidad de la Contraloría General de la República.

Toda información electrónica recibida por el equipo auditor asignado, debe ser suministrada al auditor o auditores que la solicitaron para el desarrollo de sus procedimientos de auditoría con el fin de que realicen una copia en un medio o

[9] Guías de Auditoría - CGR - Contraloria [en línea]. <http://www.contraloria.gov.co/control-fiscal/control-fiscal-micro-proceso-auditor/guias-de-auditoria > [citado en 11 de diciembre de 2017]

dispositivo diferente al que suministra la entidad en su respuesta y posteriormente devuelto al líder del equipo auditor para su conservación temporal durante el tiempo que se desarrolle la auditoría.

Cada CD o DVD generado o recibido debe contar con un rótulo en la cara provista para ello (cara opaca del medio óptico) con el fin de contar con una identificación clara que permita su reconocimiento. No se debe escribir en la cara del CD o DVD dispuesta para la grabación de datos (cara brillante del medio óptico).

Con el fin de garantizar la confiabilidad, integridad, disponibilidad y accesibilidad de la información digital o electrónica, es necesario evitar la manipulación de los medios ópticos de almacenamiento en que fueron recibidos, ya que estos representan la prueba original de los hechos evidenciados, así como la constancia de que la entidad que los origina es quien los suministró.

DESCRIPCION DEL PROCESO

La recepción, custodia y uso de la información en medios digitales debe realizarse manteniendo unos estrictos controles que ayuden a garantizar su integridad, disponibilidad y accesibilidad en cualquier momento que la misma sea requerida, permitiendo con esto que dicho soporte que forma parte del material probatorio de un hallazgo se mantenga intacto y preste el mérito suficiente dentro de los procesos asociados al mismo.

Con este propósito como fin primordial del presente manual, se presenta los pasos que deben ejecutarse dentro de las etapas de recepción, custodia y uso de la información recibida en un medio digital o electrónico, durante el desarrollo de una auditoría gubernamental programada por el Nivel Central de la Contraloría General de la República.

1. RECEPCIÓN Y/O RECOLECCIÓN DE INFORMACIÓN ALMACENADA EN MEDIO DIGITAL O ELECTRÓNICO.

La información solicitada dentro del desarrollo del proceso auditor, puede encontrarse en un medio físico o en un medio digital o electrónico.

La información recibida en medio físico cuenta con procedimientos establecidos en la guía de auditoría para su disposición, referenciación y archivo durante la etapa de ejecución de la auditoría y al terminar el proceso auditor.

La información presentada en un medio digital o electrónico requiere de un tratamiento especial que permita garantizar su identificación, organización y custodia durante el desarrollo de la auditoría que la solicita.

1.1. SOLICITUD DE INFORMACIÓN

Durante la etapa de ejecución de una auditoría, se requiere solicitar a la entidad auditada, información que, de acuerdo con los objetivos y la asignación realizada, permita realizar los análisis necesarios con el fin de evaluar la gestión y uso de los recursos asignados por el estado, conforme a la normatividad establecida para cada entidad.

La solicitud debe ser presentada por escrito o por correo electrónico, de acuerdo con los lineamientos establecidos para las comunicaciones oficiales externas en la Contraloría General de la República.

La información solicitada por los auditores como evidencia a ser analizada, para determinar el cumplimiento o no de las funciones establecidas en la Ley por parte de la entidad vigilada, deberá contar con una certificación emitida por el propietario de la misma, independiente del medio de origen y/o fuente del reporte, que garantice su procedencia, autenticidad y confiabilidad.

Toda solicitud oficial de información emitida por el equipo auditor al ente vigilado, y que deba ser suministrada en medio digital o electrónico (archivos electrónicos, reportes emitidos por productos de software institucionales, archivos digitales, y otros relacionados), deberá requerir una relación de todos los archivos electrónicos suministrados, que contenga como mínimo los siguientes datos identificadores por cada uno de ellos:

- Nombre completo del archivo electrónico, incluyendo su extensión.
- Tamaño en bytes que ocupa el archivo en el medio de almacenamiento suministrado (CD, DVD o mensaje de correo electrónico).
- Fecha de creación del archivo suministrado, incluyendo hora.
- Código HASH calculado utilizando el algoritmo MD5, para cada archivo.

Si la información se presenta en un medio óptico (CD o DVD), dicho medio debe venir rotulado, en la cara dispuesta para ello, con los siguientes datos mínimos:

- Número de oficio de solicitud del grupo auditor.
- Fecha de solicitud del grupo auditor.
- Número de oficio de respuesta de la entidad auditada.
- Fecha de respuesta de la entidad auditada.

1.2. RECEPCIÓN DE INFORMACIÓN

La información entregada por la entidad en respuesta a un requerimiento de información en medios digitales, debe contener la relación de archivos con las características de identificación mencionadas en el punto anterior. La relación requerida debe presentarse en medio impreso para los medios ópticos y en un archivo electrónico adjunto para los correos electrónicos.

Si la comunicación emitida por la entidad auditada, y que contiene información digital o electrónica, no cuenta con esta relación, debe realizarse devolución de la

información digital al ente auditado para que genere la relación correspondiente y de esta manera formalizar su entrega y recepción a cabalidad.

Si la información se presenta en un medio óptico (CD o DVD), se debe verificar que contenga la identificación rotulada en su cara conforme a las indicaciones establecidas. En caso de no contar con esta identificación, el equipo auditor debe realizarla en presencia de la persona que realiza su entrega.

Adicionalmente al cumplimiento de las formalidades en la presentación, el medio de almacenamiento recibido, y que contiene la información solicitada, debe ser revisado por el equipo auditor en el momento de su entrega y en presencia del funcionario de la entidad auditada que entrega la documentación solicitada. El medio de almacenamiento entregado, debe ser verificado en un equipo de cómputo mediante la lectura y acceso a la información almacenada en él, para garantizar que no se presenten errores que impidan su adecuada lectura y uso, y que la misma ha sido generada, grabada y/o transmitida correctamente por parte del emisor. Esta revisión es una condición necesaria y primordial para emitir el recibido a satisfacción del requerimiento realizado.

1.3. DISPOSICION DE LA INFORMACIÓN DIGITAL RECIBIDA DURANTE EL PROCESO AUDITOR.

Toda la información recibida debe ser catalogada en el formato "*Inventario de Información o Evidencia Digital recibida*" que se establece para relacionar los diferentes medios de almacenamiento recibidos durante el proceso auditor (Ver Anexo B).

Cada uno de los medios de almacenamiento de información recibido y verificado, se debe identificar por medio de la referencia establecida por la Guía de Auditoría para el oficio de respuesta emitido por la entidad vigilada.

Los medios ópticos o digitales recibidos deben ser mantenidos en sus empaques originales entregados por la entidad vigilada.

Durante el tiempo que dura la ejecución de la auditoría, es el líder del equipo auditor, el funcionario responsable de garantizar su salvaguarda y correcta conservación. Para esto, debe mantener los medios de almacenamiento conservados en sus respectivos empaques y en caso de ser CD o DVD generados a partir de archivos adjuntos a correos electrónicos, se deben guardar en un sobre de vinil de transparencia cristalina.

El equipo auditor, y su líder principalmente, deben seleccionar un lugar que permita guardar los medios de almacenamiento recibidos, asegurando su conservación y evitando su manipulación adicional. Toda información recibida, una vez confirmada su entrega con el cumplimiento de requisitos, se suministra al auditor que la solicitó o la requiere con el fin de que realice una copia para su manipulación y trabajo. Una vez realizada la copia, debe devolverse inmediatamente al archivo temporal de la auditoria para su custodia.

1.4. MEDIOS AUTORIZADOS PARA RECIBIR INFORMACIÓN DIGITAL SOLICITADA DURANTE EL PROCESO AUDITOR

La información digital recibida de la entidad como respuesta a un requerimiento del grupo auditor a la entidad vigilada, únicamente será admitida en medios ópticos como CD o DVD, o como un archivo electrónico adjunto a un mensaje de correo electrónico remitido.

Toda la información solicitada en medio digital o electrónica, por parte del equipo auditor, únicamente será válida en los siguientes medios, formatos y características:

- La información que se transmite por un medio de comunicación como el correo electrónico, deberá ser validada con los datos identificativos requeridos en la solicitud. En el caso de no corresponder con estos valores identificadores, se deberá devolver a la entidad remitente y requerir su corrección.

Si la información es correcta, la misma será grabada o archivada en un disco óptico, que puede ser DVD o CD dependiendo del tamaño, junto con los valores identificativos de los archivos.

Cada solicitud debe corresponderse con uno de estos medios, es decir, debe existir un CD o DVD por cada envío de información que la entidad realice en respuesta de una solicitud realizada por el equipo auditor.

- La información recibida directamente en CD o DVD, deberá ser comparada con sus datos identificadores, y validado su correcto funcionamiento en un equipo de cómputo.

De igual manera que un correo electrónico, de no corresponder la información con su identificación solicitada, será devuelta al remitente para su corrección.

- Para el caso de la información correspondiente a documentación que deba ser analizada en un medio digital, se aceptarán archivos en formato PDF, TIFF o JPEG.

- Para los archivos que contienen información que requiere de cálculos matemáticos, consultas de comparación, búsqueda o filtros, los formatos admitidos corresponden a hojas de cálculo en Excel, archivos planos separados por coma, archivos planos separados por punto y coma y archivos planos separados por tabulaciones.

- Toda evidencia digital que sirva como soporte para un hallazgo con incidencia fiscal, debe ser almacenada en un medio óptico como CD o DVD, debidamente rotulado y enviado para su almacenamiento en custodia. El medio óptico mencionado estará disponible para consulta o práctica de pruebas adicionales requeridas dentro de una indagación preliminar o proceso de responsabilidad fiscal.

A continuación, se presenta el diagrama de flujo correspondiente a esta etapa.

Diagrama de Flujo. Recepción o recolección de información almacenada en medio digital o electrónico.

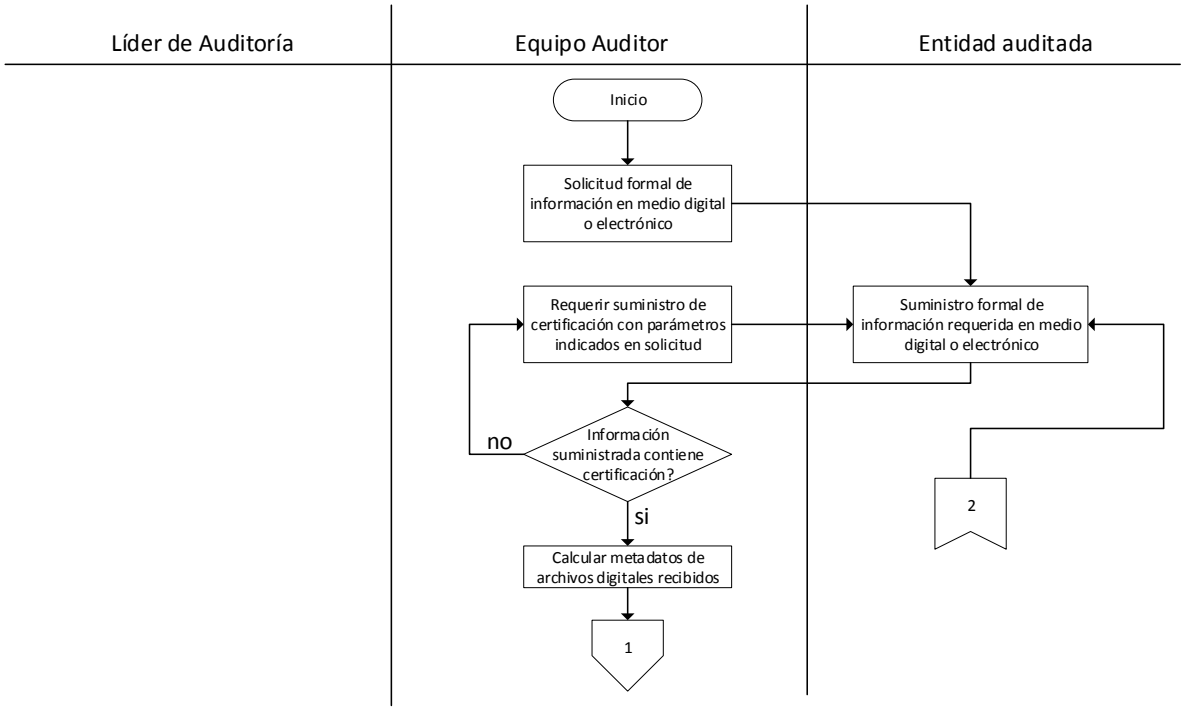
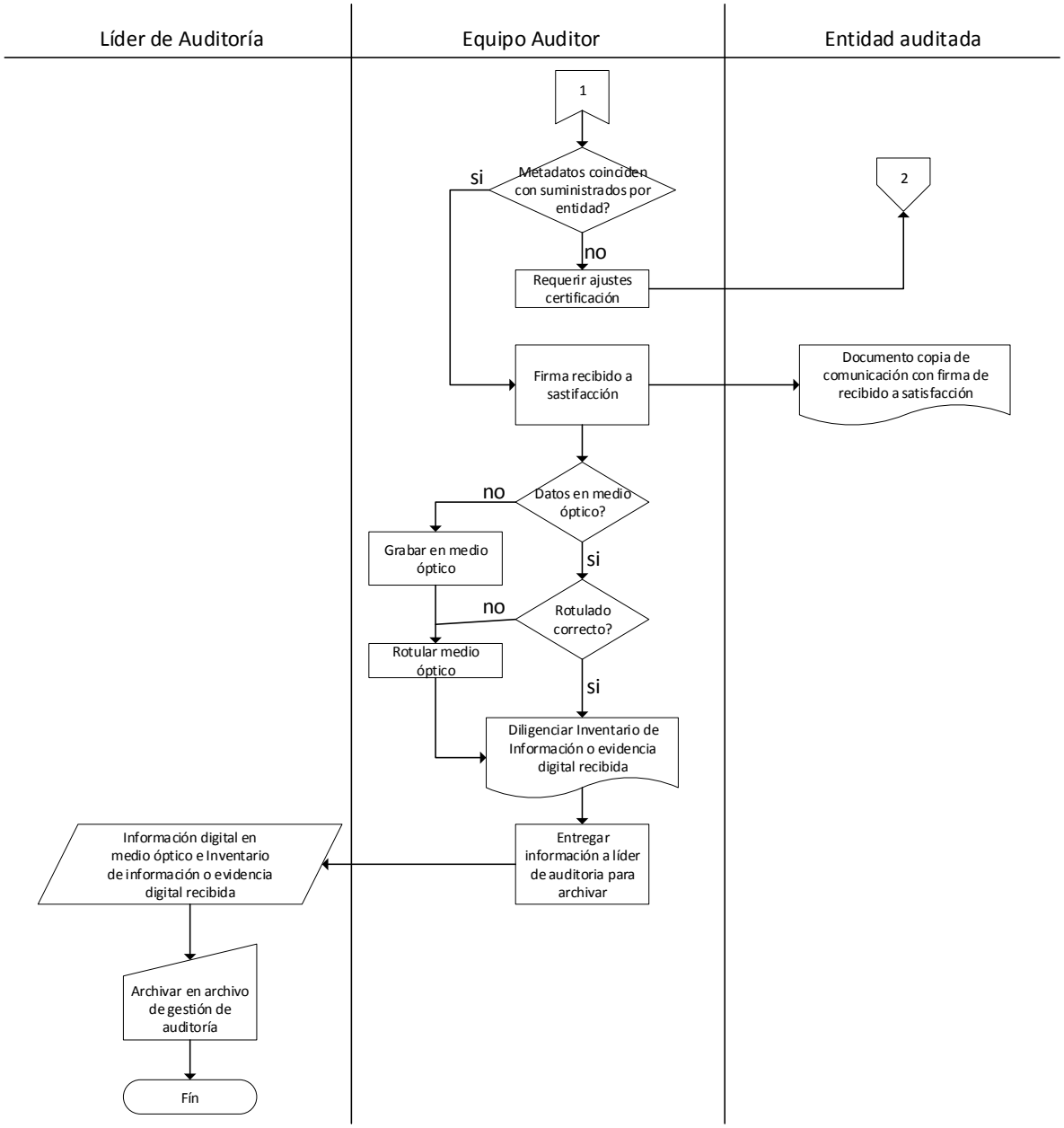


Diagrama de Flujo. Recepción o recolección de información almacenada en medio digital o electrónico. (continuación)



2. CADENA DE CUSTODIA DE INFORMACIÓN DIGITAL RECIBIDA O RECOLECTADA

Con el fin de preservar la información que compone la evidencia digital recaudada como sustento probatorio dentro de un proceso auditor, se definen los siguientes pasos a cumplir, de manera obligatoria, por parte de los equipos auditores una vez terminadas las actuaciones en las entidades asignadas.

2.1. IDENTIFICACIÓN DE LOS MEDIOS DE ALMACENAMIENTO

Todos los medios de almacenamiento (CD o DVD), recibidos o generados dentro del proceso auditor, deben venir debidamente rotulados, identificando como mínimo los siguientes datos:

- Número de oficio de solicitud del grupo auditor.
- Fecha de solicitud del grupo auditor.
- Número de oficio de respuesta de la entidad auditada.
- Fecha de respuesta de la entidad auditada.

Cada uno de los medios de almacenamiento debe ser embalado en sobres de vinil de transparencia cristalina, que permita ver su correspondiente rotulo de manera clara.

El líder del equipo auditor deberá hacer entrega formal, a la dependencia asignada para el archivo de evidencia digital recibida y mediante oficio debidamente diligenciado, de la totalidad de medios de almacenamiento recibido durante el ejercicio auditor.

La cantidad de CD o DVD, debe corresponder con la relacionada en el formato de *"Inventario de evidencia digital recibida"* (Anexo B), que se adjuntará al oficio de entrega al archivo de evidencias digitales.

2.2. ENTREGA DE MEDIOS DE ALMACENAMIENTO PARA SU ARCHIVO

El líder del equipo auditor, una vez terminada la auditoría, entregará al funcionario asignado para la gestión y administración del archivo de evidencia digital los medios de almacenamiento óptico (CD, DVD) que haya recibido o generado dentro del proceso auditor y que correspondan a evidencia en medio electrónico o digital, recolectada como soporte de los procedimientos.

La entrega de la información digital, debidamente embalada, debe realizarse mediante oficio remisorio que deberá relacionar:

- Auditoría realizada.
- Entidad auditada.
- Vigencia auditada.
- Cantidad de CD o DVD entregados a archivo de evidencia digital.

El oficio y los medios de almacenamiento deberán estar acompañados de una copia del inventario de evidencia digital recibida durante el proceso auditor, debidamente diligenciado en su totalidad y firmado por el líder del equipo auditor. Se entregará, por parte del líder, una (1) copia de dicho inventario en papel.

El paquete embalado será recibido y verificado por el funcionario asignado al archivo de evidencia digital quien comprobará la información recibida, la cantidad de medios entregados por el líder del equipo auditor, la correcta identificación de los medios y el embalaje de los mismos.

Si la revisión realizada en el momento de la entrega presenta inconsistencias, la misma será devuelta al equipo auditor para que realice las correcciones a que haya lugar. En caso contrario, el funcionario dará su visto bueno de conformidad con la información y medios recibidos, indicando la fecha y hora de la entrega correcta.

El oficio remisorio deberá contar con su correspondiente número de radicación generado por el software de uso oficial de la Contraloría General de la República, para la gestión de la correspondencia.

2.3. DISPOSICIÓN Y ARCHIVO DE MEDIOS DE ALMACENAMIENTO

Una vez recibidos a conformidad los medios de almacenamiento, el funcionario encargado de archivarlos, realizará el registro del paquete en el medio informático dispuesto para tal fin (hoja de cálculo, aplicación o software de inventario).

El registro realizado permitirá asignar un código interno de identificación del conjunto de medios de almacenamiento y una referencia geográfica de ubicación dentro del espacio determinado para la disposición de dichos medios.

El medio informático seleccionado para el registro de los medios de almacenamiento recibidos en el archivo correspondiente, deberá permitir el registro de la fecha de recibo y/o generación de los medios magnéticos, con el fin de tener un control sobre el tiempo de vida útil esperado para los CD o DVD recibidos.

Una vez recibidos, se deberá realizar una copia de seguridad de los mismos como respaldo en caso de pérdida o daño de los medios o la información almacenada en ellos, en el dispositivo o medio dispuesto para ello según estudio previo realizado. Esta copia de seguridad deberá realizarse como una imagen del medio de almacenamiento recibido.

Estos medios de almacenamiento se encontrarán a disposición de los funcionarios interesados o asignados a procesos que se generen a partir de los hallazgos detectados. Para esto, deberá contar con el respectivo documento, firmado por el directivo correspondiente, quien, en conjunto con el funcionario solicitante, serán los responsables de la salvaguarda y cuidado de los medios requeridos durante el tiempo del préstamo.

Se recomienda, salvo situaciones que lo ameriten, un tiempo máximo de dos (2) días de préstamo. Este tiempo es necesario y suficiente para que el funcionario o funcionarios asignados realicen únicamente una copia de los archivos contenidos en un medio distinto con el fin de salvaguardar el medio original que corresponde a la prueba generada o entregada por la entidad examinada y pueda ser devuelto al archivo de evidencias digitales, evitando su manipulación y posible modificación por manejo diferente al señalado.

El funcionario que recibe el medio de almacenamiento devuelto al final del préstamo por parte del funcionario que realizó la solicitud, deberá validar que dicho medio no haya sufrido afectaciones que impidan su correcta lectura y/o que se presenten condiciones que hayan modificado las características establecidas en la certificación por parte de la entidad que los suministró.

2.4. RECUPERACION DE MEDIOS DE ALMACENAMIENTO A PARTIR DE COPIAS DE SEGURIDAD

En caso de presentarse una alteración de los medios de almacenamiento archivados en custodia, y que impidan su correcta lectura, deberá informarse de dicha situación a los directivos para que ellos, mediante comunicación escrita, autoricen la creación de un nuevo medio de almacenamiento con la información almacenada como copia de seguridad en el momento de la entrega por parte del equipo auditor.

Se procede a realizar la búsqueda de la información en el dispositivo seleccionado para almacenar las imágenes obtenidas de los medios de almacenamiento recibido, para ser grabadas en un nuevo medio de almacenamiento con características iguales o similares al medio de almacenamiento original.

Esta labor será realizada por la persona encargada de custodiar el archivo y quien deberá contar con los conocimientos técnicos necesarios para la generación y restauración de imágenes de medios de almacenamiento digital como respaldo a la información recibida por los equipos auditores como pruebas y soportes de prueba de las labores realizadas.

En el diagrama siguiente se esquematiza esta etapa.

Diagrama de Flujo. Cadena de custodia de información digital recibida o recolectada en auditorías.

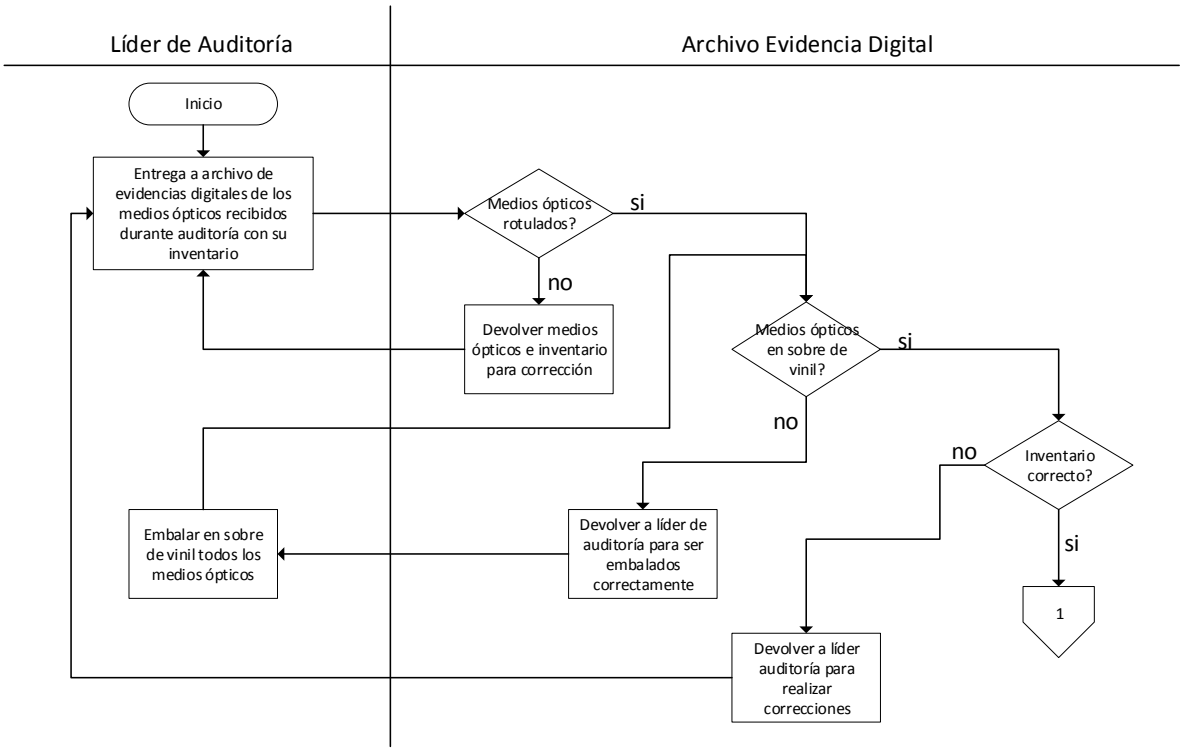
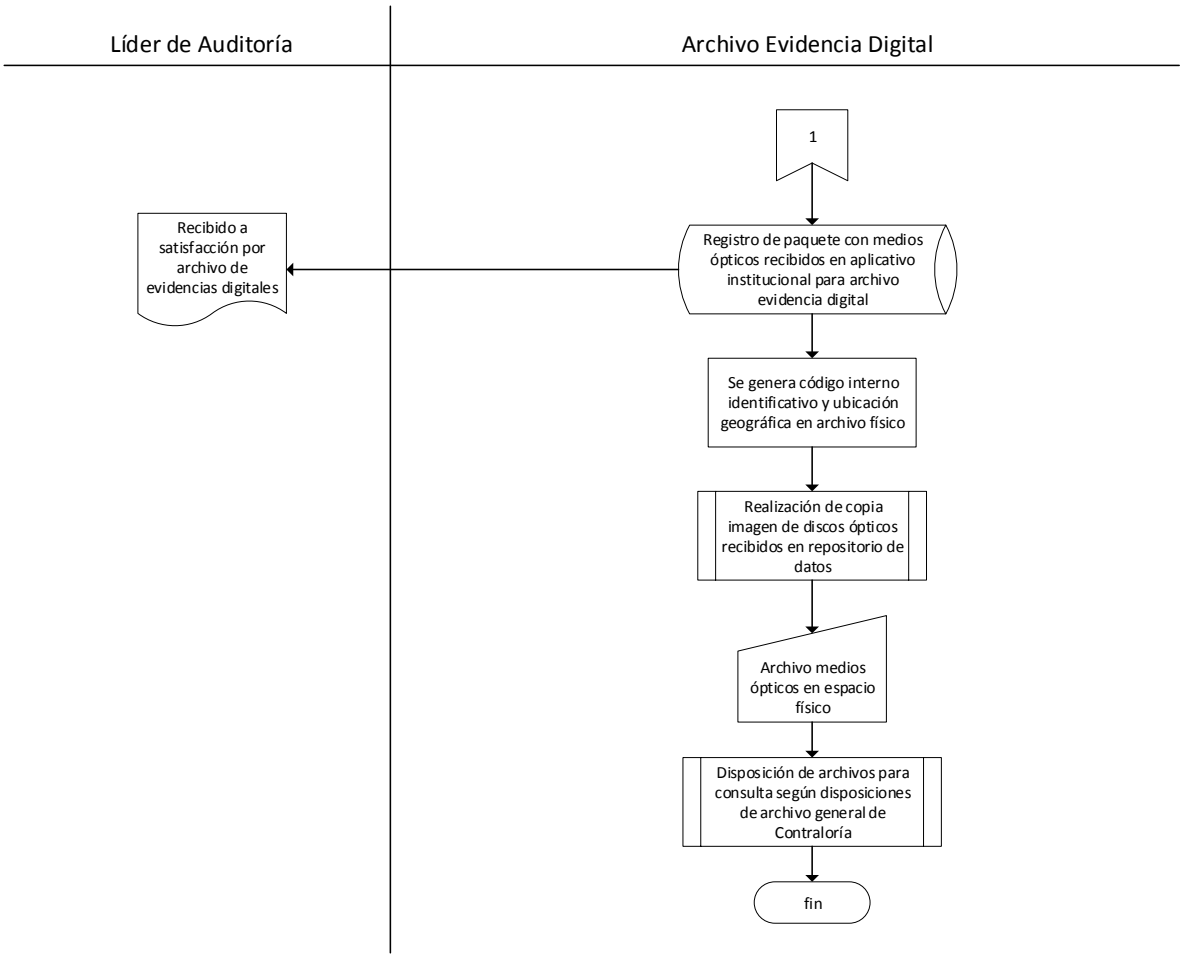


Diagrama de Flujo. Cadena de custodia de información digital recibida o recolectada en auditorías. (continuación)



3. USO Y ANÁLISIS DE INFORMACIÓN RECIBIDA EN MEDIO DIGITAL O ELECTRÓNICO.

Se determina a continuación los métodos a seguir y las herramientas oficiales que posee legalmente la Contraloría General de la República, para la realización de análisis sobre la evidencia digital recibida y la presentación de los resultados obtenidos en los procesos requeridos.

3.1. DEFINICIÓN DEL TIPO DE ANÁLISIS A REALIZAR

En esta primera fase de análisis, se determina el tipo de examen a realizar con base en la información recibida.

3.1.1. Archivos que contienen información que requiere de análisis matemático, financiero y/o contable. Corresponde a toda la información que la entidad auditada presenta y que se relaciona con sus departamentos contables y financieros.

En esta clasificación se encuentra las relaciones de cuentas, facturación, balances, presupuestos, información de gastos y toda la información que refleje la contabilidad de la entidad y la gestión de los recursos financieros que le fueron asignados de acuerdo con el presupuesto nacional.

3.1.2. Archivos que corresponden a listados y requieren de análisis estadísticos, cantidades y porcentajes. Se refiere a toda la información que se entrega en listados y que requiere ser organizada, realizar conteos por grupos conformados por un criterio determinado o relaciones de datos que requieren filtros.

En esta clasificación se encuentran los listados de información contractual, listados de elementos, listados de sedes, listados de personas, relación de contratos para ser clasificados por tipo de contratación y toda información que deba ser agrupada, clasificada y se necesite generar estadísticas y/o porcentajes para estudiar comportamientos en las gestiones.

3.1.3. Archivos que corresponden a registros de información y requieren de un análisis de datos y consultas de tipo SQL. Son todos aquellos archivos de registros de bases de datos o reportes en archivos planos generados por sistemas de información o aplicaciones de software de registro de información.

Aquí se clasifican reportes en archivo plano de sistemas de sectores salud, educación, defensa, etc., tales como Bases de datos de afiliados a sistemas de salud (contributivo y subsidiado), Bases de datos de sistemas de matrículas de instituciones educativas y Ministerio de Educación Nacional, Bases de Datos de registro de procesos judiciales, etc. Corresponde a toda aquella información que requiera ser validada con respecto a su integridad, consistencia, validez de los datos almacenados de acuerdo con la información adicional registrada.

3.2. SOLICITUD DE ANÁLISIS A REALIZAR

La solicitud es realizada por los directivos o funcionarios que requieren la ejecución de una prueba o procedimiento de perito que permita obtener los resultados deseados.

Una vez se ha determinado el tipo de prueba a realizar, se procede a realizar por medio escrito la solicitud del funcionario especialista dependiendo del tipo de procedimiento a ejecutar.

El funcionario asignado es quien realiza la solicitud de información, al archivo de evidencias digitales, de la información que requiere utilizar para ejecutar las pruebas solicitadas.

Identificado el tipo de análisis requerido, se identifica la herramienta de software adecuada.

3.2.1. Archivos que contienen información contable y requieren de análisis matemático, financiero y contable. Para este tipo de archivos, la herramienta que se adecúa a las necesidades específicas de análisis es Microsoft Excel.

Esta herramienta puede ser utilizada por la mayoría de funcionarios para realizar cálculos columnas entre datos de dicha hoja, así como operaciones que requieren de cómputos contables para establecer si las operaciones que la entidad vigilada efectuó se ajustan a los ordenamientos y lineamientos establecidos legalmente.

3.2.2. Archivos que corresponden a listados y requieren de análisis estadísticos, cantidades y porcentajes. A este tipo de información se aplica la herramienta Microsoft Excel y las funcionalidades incluidas en él, correspondientes al uso de funciones o creación de fórmulas que generen los resultados requeridos.

El uso de la herramienta, para este tipo de análisis, necesita de un funcionario con conocimientos de Excel, nivel avanzado. En caso de ser necesario debe requerirse el apoyo de un profesional con el conocimiento requerido.

3.2.3. Archivos que corresponden a registros de información y requieren de un análisis de datos y consultas de tipo SQL. Estos archivos necesitan de la realización de consultas por medio de creación de queries en el lenguaje SQL, por lo cual se utiliza el software IDEA. En caso de no disponer del software instalado en el computador o no contar con el token correspondiente y configurado, se debe usar Microsoft SQL Server Express.

Es necesario el uso de la herramienta por parte de un funcionario con conocimientos en manejo de bases de datos, lenguaje SQL e importación de archivos planos. El perfil requerido corresponde a un ingeniero de sistemas o un tecnólogo en sistemas.

3.3. EJECUCIÓN DE ANÁLISIS REQUERIDO

Una vez determinada la herramienta, es necesario establecer el procedimiento a seguir con el fin de garantizar un análisis correcto que nos ayude a obtener resultados confiables dentro del proceso auditor adelantado. Lo anterior con el fin de que dichos resultados sean consistentes con la situación examinada y tengan el peso jurídico requerido.

Independientemente del tipo de análisis y la herramienta a utilizar, se debe solicitar al líder de auditoría, el medio de almacenamiento que contiene el archivo electrónico o digital recibido y el cual será objeto del análisis. El funcionario analista de la evidencia procederá a realizar una copia del archivo o archivos que se examinarán en un disco duro interno o externo, o en un dispositivo de almacenamiento USB si dicha copia no fue realizada en el momento de recibir la información de la entidad vigilada. Una vez realizada la copia, se debe devolver el medio de almacenamiento con los archivos originales al líder para su almacenamiento temporal durante el desarrollo de la auditoría.

Si los archivos digitales que contienen la información objeto de análisis se encuentran en el archivo de evidencia digital establecido, se debe realizar solicitud a dicha área para que se suministre los medios de almacenamiento para realizar una copia en un dispositivo o medio diferente (los medios establecidos para la información que se encuentra en auditoría) y posteriormente devolver el medio original a dicho archivo en el tiempo establecido.

Los procedimientos de análisis que se deben ejecutar, de acuerdo con el tipo de análisis y la herramienta requerida, son:

3.3.1. Archivos que contienen información contable y requieren de análisis matemático, financiero y contable con Microsoft Excel. El primer paso a verificar es que el archivo recibido se encuentre en un formato compatible con Microsoft Excel (una hoja de cálculo de Excel, archivo plano, archivo de texto, otros orígenes permitidos).

En primera instancia se debe realizar una copia del archivo recibido, con el fin de no afectar la información inicialmente recibida para el caso de comprobar que corresponde al remitido por el auditado. Los medios ópticos originales se deben

devolver al archivo de evidencias digitales quien registra la devolución y procede a archivar nuevamente los medios en la ubicación determinada en el registro correspondiente del aplicativo institucional.

Posteriormente, se ejecuta el software correspondiente, en este caso una hoja de cálculo (Microsoft Excel) y se procede a abrir el archivo recibido.

Si el formato del archivo recibido corresponde a un libro de Excel, se procede a abrir dicho archivo mediante la opción abrir de la herramienta. Si el archivo pertenece a otro formato diferente, se debe importar mediante el asistente encontrado en la opción Datos del menú de Microsoft Excel.

El archivo abierto en Microsoft Excel, debe ser guardado con un nombre diferente, al corresponder con un archivo de trabajo, a partir del cual se realicen los cálculos correspondientes.

El analista del archivo o archivos recibidos, procede a establecer los cálculos que se desea verificar con el fin de obtener los resultados esperados.

Determinadas las operaciones necesarias, en una nueva hoja de cálculo, se procede a copiar los datos que se requieren para el análisis y se digitará la fórmula o fórmulas que el analista ha determinado para obtener los resultados. Es posible seleccionar fórmulas ya diseñadas, si las mismas se ajustan a los requerimientos de análisis de la auditoría.

Estas labores se realizan sobre la copia del archivo recibido para evitar manipulación de la información original recibida que cuenta con la certificación generada por parte del emisor, que garantiza que la misma fue obtenida de acuerdo con las condiciones normativas establecidas para la Contraloría General de la República.

3.3.2. Archivos que corresponden a listados y requieren de análisis estadísticos, cantidades y porcentajes. De igual forma que el ítem anterior, se debe realizar como primer paso, la apertura o la importación del archivo recibido, dependiendo del formato en que se encuentre.

Acto seguido se procede a copiar los datos que se requieren en el análisis deseado y posteriormente, se inserta o crea la fórmula que, de acuerdo con el objetivo planteado y los resultados esperados, permitirá realizar el análisis de manera objetiva y puntual, siempre apoyada en los criterios o normas que establecen el cómo se debe gestionar los recursos en cada entidad.

3.3.3. Archivos que corresponden a registros de información y requieren de un análisis de datos y consultas de tipo SQL. Para este caso, la herramienta de software IDEA, cuenta con un asistente de importación en el cual se puede seleccionar el formato en el cual se encuentra grabado o digitalizado el archivo recibido como evidencia solicitada.

El analista, que en este caso es un funcionario con perfil y conocimientos en sistemas de información y bases de datos, procede a examinar los campos contenidos en el archivo, y la organización y delimitación de campos del mismo.

Una vez determinados los campos, se ejecuta la consulta o las consultas que sean necesarias conforme al objetivo de auditoría o los lineamientos establecidos por el equipo auditor de acuerdo con el procedimiento diseñado y desarrollado.

En caso de requerir confrontación de información con otra fuente o la comparación con otro archivo, dicha fuente o archivo adicional debe ser requerido por el líder de la auditoría en los términos y con las condiciones establecidas en el punto de recolección de evidencia digital.

En este punto es importante aclarar que sí, el funcionario analista no pertenece al equipo auditor, la solicitud de análisis debe ser presentada al Supervisor de Auditoría y/o el Ejecutivo de Auditoría, estableciendo el tipo de información recibida, los objetivos planteados, los resultados esperados y los tiempos establecidos para presentar el examen ejecutado. Este requerimiento debe realizarse mediante un escrito conforme a los lineamientos establecidos en la Gerencia Departamental para la elaboración y envío de comunicaciones oficiales internas, el cual debe contemplar como mínimo:

- Relación de la información a ser analizada.
- Objetivos planteados o requerimientos del análisis.

3.4. ENTREGA DE RESULTADOS OBTENIDOS

Una vez los análisis han sido llevados a cabo en su totalidad, el funcionario encargado de realizar dicho examen debe diligenciar el Reporte de presentación de resultados de análisis de evidencia digital, especificado en el anexo C del presente documento.

En primera instancia se debe validar que la información de los metadatos suministrados por la Entidad como certificación, correspondan a los calculados por el funcionario asignado para rendir el reporte de resultados.

Una vez validada la información a evaluar, se procede a realizar la ejecución del procedimiento de acuerdo con el tipo de información y la prueba solicitada.

Este documento debe diligenciarse en su totalidad. En caso de que el análisis sea realizado por un funcionario miembro del equipo auditor, el campo correspondiente al oficio de solicitud del análisis debe diligenciarse con la frase: “No aplica, funcionario analista es miembro del equipo auditor”.

Si el análisis fue ejecutado por un profesional que no forma parte del equipo que adelanta el proceso auditor, dicho reporte debe remitirse al líder del equipo auditor, o al supervisor de auditoría mediante comunicación oficial diligenciada y registrada de acuerdo con el procedimiento establecido por la Contraloría General de la República para el envío de comunicaciones oficiales internas.

A continuación, se puede apreciar de manera gráfica, el desarrollo de esta etapa.

Diagrama de Flujo. Uso y análisis de información recibida en medio digital o electrónico.

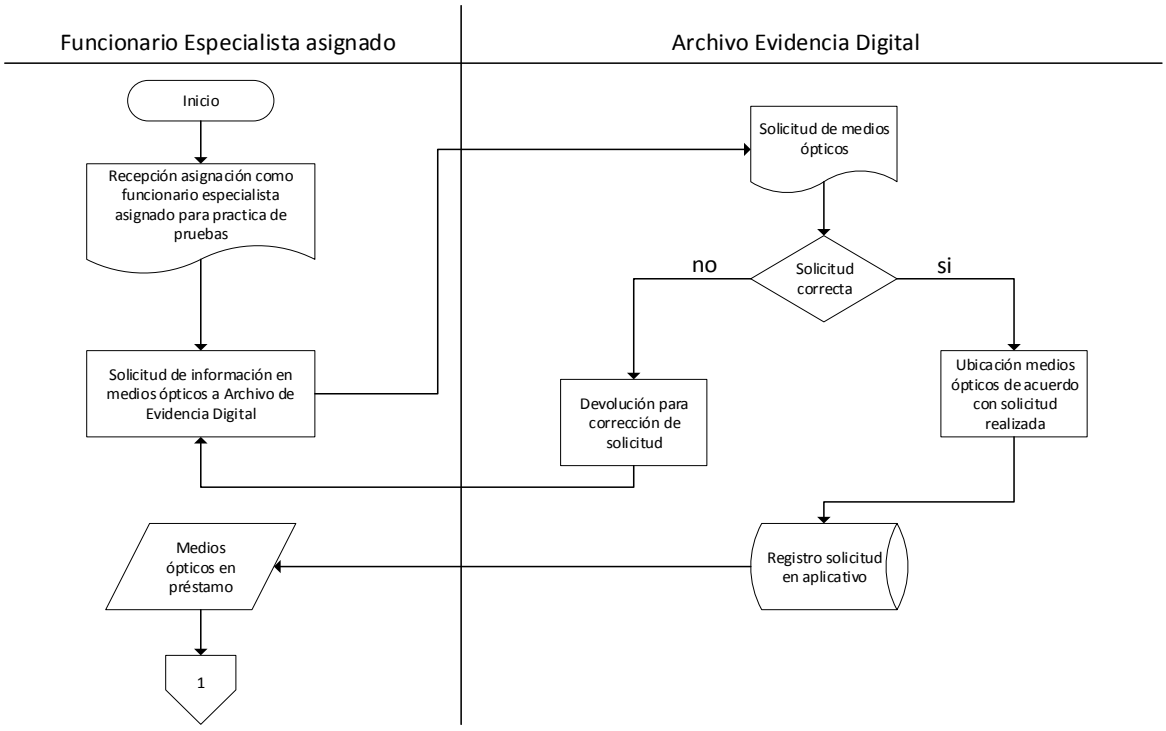
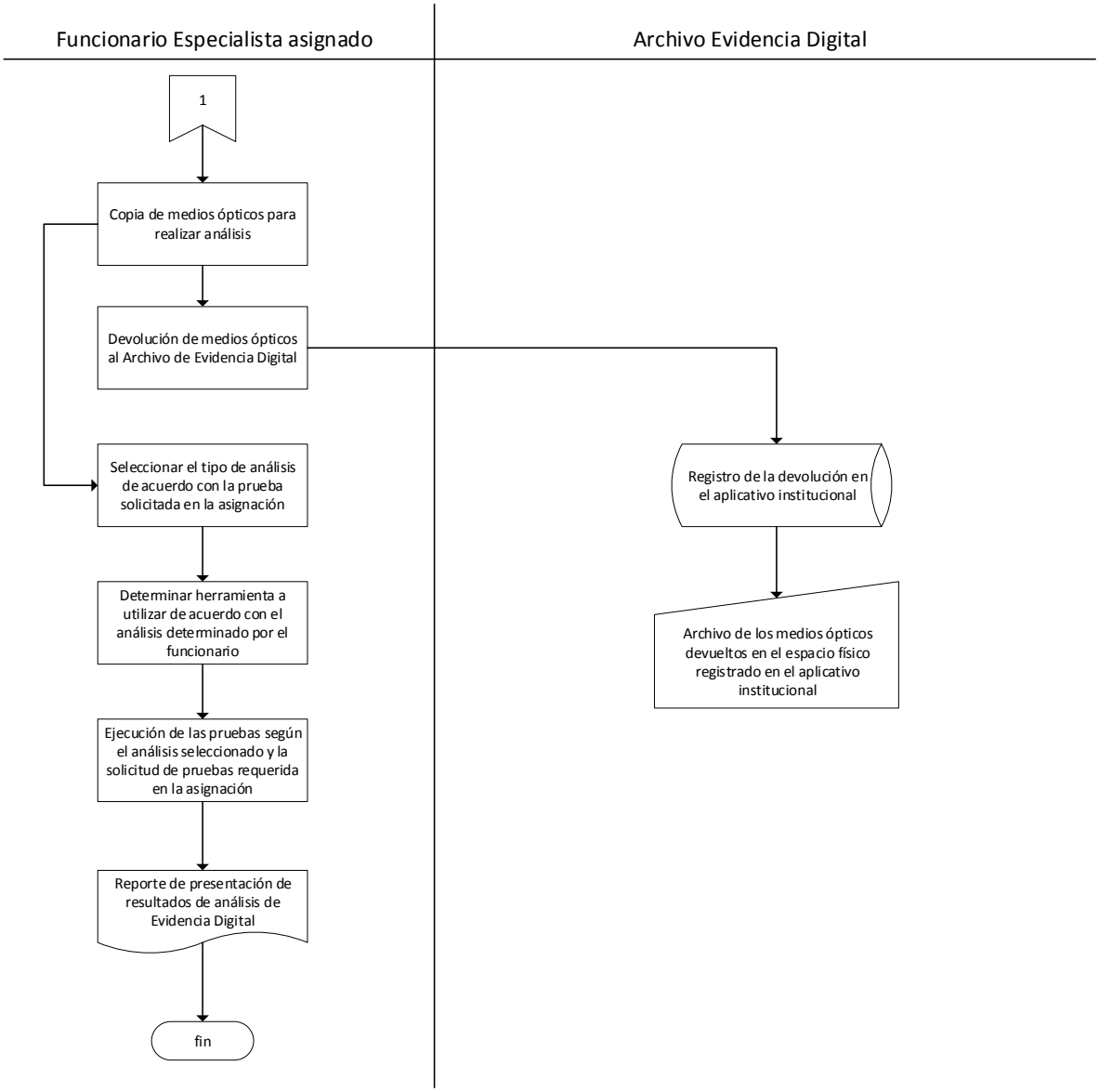


Diagrama de Flujo. Uso y análisis de información recibida en medio digital o electrónico. (continuación)



RESPONSABLES

Supervisor de Auditoría: Es la persona encargada de la vigilancia del desarrollo de las actividades y procedimientos realizados dentro de una auditoría.

Se encarga de verificar que los procedimientos y lineamientos establecidos en las guías, manuales y normas correspondientes se cumplan correctamente.

Líder del Equipo Auditor: Es el funcionario, miembro del equipo auditor, que se ha designado para dirigir, controlar y supervisar las actividades dentro del equipo auditor.

Para este procedimiento, tiene la responsabilidad de verificar que la información digital sea solicitada y suministrada cumpliendo los lineamientos establecidos y además de garantizar su correcta custodia.

Auditor(es): Son los funcionarios que se han asignado al equipo para realizar las labores de auditoría de acuerdo con su perfil profesional.

Tienen a cargo la solicitud y uso adecuado de la información digital recibida, así como de la realización de análisis o requerimientos a otros profesionales expertos en análisis de bases de datos.

Funcionario Archivo de Evidencias digitales: Este funcionario es designado por los directivos y tiene como función, la de recibir, organizar y controlar la información digital recibida durante los procesos auditores, así como su correcta disposición, garantizando su conservación y salvaguarda como material probatorio.

Funcionario Especialista análisis de bases de datos: Es el funcionario que, de acuerdo con su perfil profesional, tiene los conocimientos y aptitudes necesarias para realizar análisis a bases de datos.

Este funcionario, que por lo general es un ingeniero de sistemas, debe disponer de la información para la realización de análisis y estudios correspondientes para entregar los resultados solicitados.

REFERENCIAS

CALAMEO. Guía para el manejo de evidencia digital [en línea]. <http://es.calameo.com/read/004053479c7bcc08c68de> [citado en 26 de octubre de 2015]

CANO, J. Introducción a la informática forense. En: Sistemas. no. 96, p. 64-73.

CANO MARTINEZ, Jeimy J. Computación forense. Descubriendo los rasgos informáticos. México, D.F.: Alfaomega, 2009. 344p. ISBN 978-958-682-767-6.

MINISTERIO DE DEFENSA. Soporte legal de la evidencia digital en un incidente informático. [En línea]. <http://www.colcert.gov.co/sites/default/files/evidencia_digital.pdf> [citado en 24 de octubre de 2015]

GLOSARIO

ARCHIVO ELECTRÓNICO O DIGITAL: Es todo archivo que se genera, procesa o utiliza en un dispositivo electrónico como un computador, servidor u otros relacionados y que debe ser guardado en un medio de almacenamiento digital.

CODIGO HASH: Es un código alfanumérico que se obtiene mediante la aplicación de funciones y uso de algoritmos ejecutados sobre un archivo. Permite establecer un código único para cada archivo con el fin de garantizar su integridad y controlar la realización de modificaciones a los mismos.

MD5: Algoritmo computacional que permite realizar cálculos matemáticos de acuerdo con los datos contenidos en un archivo, para generar un valor que lo identifica como único.

MEDIO DE ALMACENAMIENTO DIGITAL: Son los soportes físicos tales como CD, DVD, Pendrive USB, tarjetas SD y otros similares que permitan guardar archivos digitales o electrónicos para ser compartidos o transportados.

PENDRIVE USB: es un dispositivo de hardware que permite el acopio y almacenamiento de información digital o electrónica como imágenes, música, documentos, entre otros. Su conexión se realiza por medio de puertos USB.

SQL: (Structured Query Language) Es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ellas, tales como consultas, comparaciones y otros.

TOKEN: Dispositivo de hardware similar a un pendrive USB que permite el almacenamiento de información de seguridad como usuarios, claves, seriales y otros para el uso de software o equipos de cómputo sin tener que digitar dicha información de autenticación.