



Ministerio
Secretaría
General de la
Presidencia

Gobierno de Chile



DOCUMENTO TÉCNICO N° 130

Versión 0.1

ASPECTOS FUNDAMENTALES SOBRE LA EVIDENCIA DE AUDITORÍA

Este documento técnico proporciona una guía integral sobre la evidencia de auditoría en el contexto de la auditoría interna del sector público chileno. A través de un análisis detallado de los principios y normas que rigen la obtención y evaluación de la evidencia, incluyendo las Normas Globales de Auditoría Interna del IIA, así como los estándares, leyes y mejores prácticas aplicables en el ámbito de la auditoría, se busca equipar a los auditores con conocimientos para realizar su labor de manera efectiva y objetiva.



DICIEMBRE 2024

TABLA DE CONTENIDOS

MATERIAS	PÁGINA
PRESENTACIÓN	3
I. INTRODUCCIÓN	4
1.1. Propósito del documento	4
1.2. Importancia de la comprensión técnica de la evidencia para la auditoría	4
II. CONTEXTO Y ALCANCE	6
2.1. Descripción de la problemática	6
III. ASPECTOS CONCEPTUALES Y NORMATIVOS DE LA MATERIA	8
3.1. Definiciones	8
IV. ACERCA DE LA “VERDAD” EN EL PROCESO DE AUDITORÍA	10
4.1. Los criterios de verdad	10
4.2. El camino hacia “la verdad” en un proceso de auditoría	16
V. CARACTERÍSTICAS, TIPOLOGÍA Y LIMITANTES DE LA EVIDENCIA EN LA LABOR DEL AUDITOR	18
5.1. Naturaleza de la evidencia en auditoría	18
5.2. Características de la evidencia en auditoría	19
5.3. Decisiones sobre la evidencia de auditoría	24
5.4. Tipos de evidencia en auditoría	25
VI. EL ESTÁNDAR DE LA EVIDENCIA EN LA AUDITORÍA INTERNA	33
6.1. El cambio conceptual: de “evidencia” a “información”	34
6.2. Importancia de la evidencia en la auditoría interna	34
6.3. Recolección y análisis de información en la auditoría interna	35
6.4. Uso y protección de la información	35
6.5. Documentación y comunicación de resultados	36
6.6. Consideraciones prácticas para los auditores internos	36
VII. EL VALOR PROBATORIO DE LA EVIDENCIA DE AUDITORIA EN UN JUICIO	37
7.1. Concepto y objeto de la prueba	38
7.2. Valoración de la evidencia: La regla de la sana crítica	42
7.3. El rol del auditor en un juicio	43
7.4. Los indicios y la prueba indiciaria en la función del auditor	46
VIII. ASPECTOS FUNDAMENTALES DE LA EVIDENCIA DIGITAL	49
8.1. Definición de evidencia digital	49
8.2. Aspectos legales esenciales sobre la evidencia digital	51

8.3. Modelos de análisis de informática forense	53
8.4. Análisis de informática forense más recurrentes	56
8.5. La evidencia digital en auditoría interna	58
8.6. Buenas prácticas para el manejo de evidencia digital en auditoría interna	59
8.7. Algunas consideraciones prácticas en manejo de la evidencia digital	60
8.8. Competencias de los auditores gubernamentales para la obtención de evidencia electrónica de auditoría	62
IX. EJEMPLOS DE CASOS PRÁCTICOS FOCALIZADOS	64
9.1. Diferencia entre evidencia y prueba	64
9.2. Cuando el auditor está en estrados	69
VII. APÉNDICE: Principios generales para la evidencia digital	73
VII. BIBLIOGRAFÍA	77

PRESENTACIÓN

En cumplimiento de las instrucciones del Presidente de la República, Gabriel Boric Font, sobre fortalecimiento de la Política de Auditoría Interna de Gobierno; el Consejo de Auditoría Interna General de Gobierno (CAIGG), entidad asesora del Supremo Gobierno en materias de auditoría interna, control interno, probidad, gestión de riesgos y gobernanza, presenta a la Red de Auditoría Gubernamental, el *Documento Técnico N° 130 titulado “Aspectos Fundamentales sobre la Evidencia de Auditoría”, versión 0.1.*

El propósito de este documento técnico es proporcionar una guía integral sobre la evidencia de auditoría en el contexto de la auditoría interna del sector público chileno. A través de un análisis detallado de los principios y normas que rigen la obtención y evaluación de la evidencia, incluyendo las Normas Globales de Auditoría Interna, así como los estándares, leyes y mejores prácticas aplicables en el ámbito de la auditoría, se busca equipar a los auditores con las herramientas necesarias para realizar su labor de manera efectiva y objetiva.

Este documento también pretende fomentar una comprensión más profunda de la importancia de la evidencia durante el proceso de auditoría interna; de este modo, la correcta aplicación de las normas no solo asegura la calidad y fiabilidad de la evidencia recopilada, sino que también promueve la transparencia y la rendición de cuentas en la gestión pública. Al adoptar un enfoque sistemático y disciplinado en la obtención de información, los auditores pueden garantizar que sus hallazgos y recomendaciones estén fundamentados en datos sólidos y verificables, lo que resulta esencial para la toma de decisiones informadas y para el fortalecimiento de la gobernanza en el sector público.

Santiago, diciembre de 2024.



Daniella Caldana Fulss
Auditora General de Gobierno

I. INTRODUCCIÓN

1.1. *Propósito del documento*

En el contexto actual del sector público chileno, la función de auditoría interna se erige como un pilar fundamental para garantizar la transparencia, la rendición de cuentas y la eficiencia en la gestión de los recursos públicos. La evidencia de auditoría, en este sentido, juega un papel crucial, ya que no solo respalda las conclusiones y recomendaciones de los auditores, sino que también fortalece la confianza de la ciudadanía en las instituciones gubernamentales.

Este documento se adentra en los aspectos fundamentales de la evidencia de auditoría, destacando su importancia y relevancia en el proceso de auditoría interna. A través de un enfoque sistemático y disciplinado, se busca proporcionar a los auditores las herramientas necesarias para obtener información confiable y de calidad, lo que a su vez permitirá emitir juicios objetivos y fundamentados.

Al abordar la complejidad de la evidencia y su relación con el escepticismo profesional, se abre un espacio para la reflexión y el aprendizaje continuo, promoviendo así una cultura de mejora en la práctica de la auditoría. Con un compromiso renovado hacia la excelencia, este documento invita a los profesionales del área a explorar y aplicar los conceptos presentados, contribuyendo al fortalecimiento de la auditoría interna en el sector público chileno y, al interés público, entendido como la promoción del bienestar social, económico y general de la ciudadanía y de las organizaciones públicas que la componen.

Por otro lado, a diferencia de otros recursos técnicos, el presente documento incorpora aspectos sobre la evidencia en el ámbito judicial, como una forma de asociar conceptos y roles que quizás puedan ser desconocidos para el auditor interno, pero que son relevantes para su ejercicio profesional. Además, el perfeccionamiento de las leyes sobre probidad administrativa y delitos funcionarios exige que los auditores internos comprendan su rol ante los tribunales de justicia, en caso de que el resultado de su trabajo lo requiera.

En ese mismo orden de ideas, se han incorporado y cubierto aspectos de la “evidencia digital”, un tema delicado por naturaleza. Aunque el auditor interno no es responsable de peritar los dispositivos electrónicos ni su contenido, es fundamental que conozca ciertos procedimientos que permitan manipularlos adecuadamente sin comprometer la integridad de la información que contienen.

1.2. *Importancia de la comprensión técnica de la evidencia para la auditoría*

La importancia de la evidencia en cualquier estudio o disciplina es fundamental para la demostración de “algo”. Como se verá más adelante, no es suficiente establecer “nuestra verdad” a partir de creencias o emociones sin un respaldo adecuado. De hecho, Mautz y Sharaf ¹- referentes en este campo - nos advertían que las hipótesis que desarrollamos, ya sea en nuestras actividades cotidianas o con algún enfoque científico, solo se vuelven

¹ MAUTZ, R.K. & SHARAF, HUSSEIN A., 1961, “The Philosophy of Auditing”, 18 Edition, American Accounting Association, Estados Unidos.

suficientemente fuertes para justificar la creencia en ellas si están debidamente respaldadas por “evidencia”. Por ello, la evidencia nos proporciona una base racional para formar juicios, sobre la cual el auditor sustenta sus conclusiones.

En efecto, un auditor competente necesita pruebas para poder “juzgar” de manera racional. Tradicionalmente, el enfoque de un auditor es emitir juicios y formar una “opinión” basada en pruebas adecuadas, actuando de forma racional y siguiendo un procedimiento sistemático o metódico. Por lo tanto, si el auditor no reúne suficiente y relevante material probatorio o no lo evalúa eficazmente, estaría actuando de manera irracional, y sus juicios podrían carecer de valor. Además, no debe olvidarse que en ese proceso, los sesgos cognitivos podrían influir en su toma de decisiones.

Siguiendo a Mautz y Sharaf, la evidencia, en un sentido amplio, puede clasificarse en tres categorías: evidencia natural, evidencia creada y argumentación racional, las que están alineadas con lo establecido por Mans, como se explicará más adelante.

La primera, la evidencia natural, existe a nuestro alrededor y comúnmente confiamos en ella en cada actividad mental que realizamos. Una mesa, por ejemplo, es su propia evidencia de existencia. Vemos un inventario de cosas y estamos convencidos de que existen. Como se enfatizará más adelante, la evidencia natural es una de las más convincentes que tenemos.

La segunda, la evidencia creada, requiere un proceso previo. Esta evidencia no existe naturalmente en el mundo que nos rodea; se necesita algún esfuerzo para revelarla. Cuando un científico, por ejemplo, realiza un experimento, está creando evidencia. El agua es evidencia de su propia existencia en la naturaleza, y podemos aprender mucho sobre sus características físicas observándola inteligentemente. Sin embargo, se puede aprender aún más mediante experimentos de laboratorio, como analizar sus componentes o someterla a diferentes presiones (por ejemplo, examinar sus características hidráulicas, calentarla, enfriarla y someterla a otros procedimientos analíticos). En el primer caso, la evidencia está naturalmente disponible; en el segundo, debe ser elaborada o desarrollada científicamente por alguien con las competencias necesarias para observar los fenómenos de manera profesional, con el fin de sacar el máximo provecho de las pruebas disponibles.

De este modo, la validez de muchas hipótesis puede ser probada de forma rápida y sencilla. Quienes cuestionen los resultados de tales experimentos pueden repetirlos en condiciones idénticas. Esta adaptabilidad al método científico permite que un campo de estudio se desarrolle más rápidamente y con mayor autoridad que otros.

Por último, el tercer tipo de evidencia es la argumentación racional. Mautz y Sharaf nos enseñan que gran parte de lo que creemos no proviene directamente de la observación de evidencia natural o creada. A menudo, las ideas se derivan lógicamente de los hechos observados, lo que nos lleva a pensar que son “verdaderas”. Sin embargo, también se requiere un esfuerzo mental para pasar de la simple observación a la conclusión, un proceso que nuestras mentes encuentran interesante.

En procedimientos judiciales, por ejemplo, un abogado hábil puede desarrollar un caso “extremadamente convincente” basado en una serie de hechos establecidos y una considerable cantidad de “racionalización”. La expresión común “parece lógico” refleja con qué frecuencia nos apoyamos en este tipo de evidencia.

En conclusión, las tres grandes categorías de evidencia identificadas por estos autores no son igualmente convincentes para la mente humana. Es muy difícil para cualquiera de nosotros negar la existencia de objetos físicos (como el ejemplo de la mesa), a menos que el observador tenga problemas de visión, una identificación incorrecta u otros errores de este tipo. La evidencia de su existencia - la propia mesa - es sumamente convincente. Nuestras mentes se ven prácticamente obligadas a creer; como dijo Santo Tomás, “ver para creer”, aunque un astrónomo podría tener un enfoque diferente para aceptar lo que observa.

Por consiguiente, en la medida en que la evidencia creada sea simple y clara, puede ser igualmente convincente. Sin embargo, se requiere un proceso complejo de desarrollo: lo que no podemos comprender tendemos a rechazarlo, como ocurre con los largos y complicados procesos de racionalización matemática a gran escala. Lo mismo sucede con la argumentación racional. Si consta de uno o dos sencillos pasos de razonamiento, es más fácil de entender y estamos inclinados a aceptarla. No obstante, el factor decisivo no es la solidez de los argumentos presentados, sino el testimonio de quien los respalda. Esto no es muy diferente al trabajo que realiza un auditor

II. CONTEXTO Y ALCANCE

2.1. Descripción de la problemática

Varias publicaciones académicas se han enfocado en explicar las razones detrás de las deficiencias de los auditores al realizar auditorías financieras. Junto a estas investigaciones, se han sumado otras de tipo empírico, centradas en el desempeño de los auditores ante la US Securities and Exchange Commission (SEC). Entre estos estudios destaca el conducido por Beasley (North Carolina State University) et al., cuyos resultados fueron publicados en 2013².

Las cinco principales áreas deficitarias por las que los auditores externos fueron sancionados por la SEC fueron:

1. Falta de obtención de evidencia de auditoría suficiente y competente (73% de los casos. Cabe destacar que un estudio similar realizado en 2000 arrojó un 80%).
2. No ejercer el debido cuidado profesional (67%).
3. Nivel insuficiente de escepticismo profesional (60%).
4. Falta de obtención de evidencia adecuada relacionada con las representaciones de la dirección de la entidad auditada (54%).
5. Falta de expresión de una opinión de auditoría adecuada (47%).

² BEASLEY, MARK S., CARCELLO, JOSEPH, HERMANSON, DANA & NEAL.TERRY, 2013, “An Analysis of Alleged Auditor Deficiencies in SEC Fraud Investigations: 1998–2010”, Estados Unidos. Funding for this research project was provided by the Center for Audit Quality.

En lo concerniente a la obtención de evidencia, ese estudio resaltó que³:

- La capacidad para diseñar y llevar a cabo procedimientos de auditoría que aborden los riesgos de incorrección material debido al fraude depende de la ejecución conjunta del debido cuidado profesional, el mantenimiento de un nivel suficiente de escepticismo profesional y la identificación y evaluación de riesgos. Es decir, el debido cuidado profesional, el escepticismo profesional y la evaluación de riesgos son condiciones necesarias para diseñar y ejecutar respuestas adecuadas a los riesgos de auditoría.
- En algunos de los casos analizados en este estudio, el auditor no realizó procedimientos de auditoría que generalmente se esperan en cualquier auditoría, como el envío de confirmaciones a terceros, la obtención de evidencia para respaldar las estimaciones, o la corroboración de las representaciones verbales de la actividad bajo revisión. En otros casos, el auditor no ajustó los procedimientos de auditoría considerando las condiciones de riesgo documentadas, limitándose a aplicar un programa de auditoría genérico o procedimientos similares a los de años anteriores. Estos hallazgos sugieren, como en el caso anterior, que puede haber dificultades relacionadas con la falta de debido cuidado profesional o el mantenimiento de un nivel suficiente de escepticismo profesional.

El estudio también ofreció ejemplos que demostraron la falta de obtención de evidencia de auditoría suficiente y competente, tales como:

1. La actividad bajo revisión manifestó haber realizado un análisis exhaustivo de los saldos de inventario, explicando las diferencias físicas. Sin embargo, el auditor confió excesivamente en los informes proporcionados por la entidad sin verificar su confiabilidad (sesgo de exceso de confianza).
2. El auditor no respaldó las estimaciones subyacentes utilizadas para establecer los saldos de los estados financieros y no obtuvo evidencia adicional cuando se identificaron posibles sesgos en su determinación por parte de la actividad bajo revisión.
3. El auditor no pudo fundamentar los precios utilizados en el cálculo de la valoración de intangibles (por ejemplo, software).
4. El auditor no realizó procedimientos adicionales cuando las confirmaciones enviadas contenían información ambigua. En esa misma auditoría, el auditor tampoco obtuvo evidencia que respaldara la estimación por obsolescencia de inventario, ni fundamentó el cálculo de los ingresos, basándose únicamente en los testimonios proporcionados por la actividad bajo revisión.

En correlación con estos hallazgos, el informe a las Naciones 2024”de la ACFE señaló que la forma más común en que se descubrieron fraudes fue a través de denuncias anónimas (canales de denuncia), lo cual representó el 43% de los casos, más del triple en comparación con otros métodos de detección. Este hallazgo es consistente con

³El lenguaje utilizado para describir estos hallazgo no representa necesariamente una cita exacta del texto original.

estudios anteriores de la ACFE, que han mostrado una tendencia similar en la revelación de fraudes. Otros métodos comunes de detección incluyeron la auditoría interna (14%) y la revisión de la dirección (13%). En conjunto, estos tres métodos representaron el 70% de los casos cubiertos por el estudio.

III. ASPECTOS CONCEPTUALES Y NORMATIVOS DE LA MATERIA DE LA MATERIA

En el presente capítulo se desarrollan los principales conceptos abordados en este Documento Técnico, con el propósito de guiar al lector a través de las dimensiones terminológicas tratadas en los distintos apartados.

3.1. Definiciones

- a) **Evidencia:** En términos generales, se entiende como la “certeza clara y manifiesta de la que no se puede dudar” (RAE, 2024). Sin embargo, es un concepto complejo, especialmente cuando la “evidencia” es relevante tanto para el auditor como para los sistemas de persecución penal y judicial, además de otras instancias que, aunque no formen parte directa del quehacer del auditor, pueden afectar su trabajo en algún momento.

Como se verá más adelante, la “evidencia” es una manifestación de una “verdad”, que responde a la pregunta “¿cómo lo sabes?”. Por otro lado, algunos teóricos sugieren que la “verdad” y el método para obtenerla no son absolutos, argumentando que ningún conocimiento, método o teoría es superior a otro, y que, por lo tanto, la “evidencia concluyente” no existiría⁴. En este sentido, las Normas de Auditoría Externa nos recuerdan que “...una seguridad razonable no significa un grado absoluto de seguridad, debido a que existen limitaciones inherentes a la auditoría que hacen que la mayor parte de la evidencia de auditoría a partir de la cual el auditor alcanza conclusiones y en la que basa su opinión sea más convincente que concluyente” (NIA Sección AU 200.5).

Existen múltiples enfoques teóricos que nos ayudan a comprender mejor la naturaleza de la evidencia con la que trabaja un auditor, cuyas raíces son más filosóficas. No obstante, como se ha mencionado, la evidencia rara vez es concluyente, pero esto no debe interpretarse como una limitación en la práctica. Por el contrario, cuanto más tipos de evidencia se encuentren en apoyo de una proposición (premisas), más probable será que dicha proposición sea cierta. En otras palabras, si logramos reunir más de un tipo de evidencia de auditoría y ninguna de ellas entra en conflicto entre sí, la probabilidad de que la proposición sea errónea disminuye considerablemente, haciendo que la suma total de la evidencia sea casi concluyente (aunque más bien “persuasiva”).

⁴ CARDOZO BRUM, MYRIAM, 2021, “Evidencia: conceptos y usos en la evaluación de políticas y programas públicos”, Iztapalapa. Revista de ciencias sociales y humanidades, México, <https://doi.org/10.28928/ri/902021/aot3/cardozobrumm>.

En este contexto, Mautz y Sharaf enfatizan dos puntos clave. Primero, no se trata solo de la cantidad de evidencia, sino de que la forma en que se obtiene varíe en su naturaleza y cubra todas las posibilidades para alcanzar el conocimiento buscado (“la verdad”). En segundo lugar, hay una gran diferencia entre una situación en la que un tipo de evidencia simplemente no puede obtenerse y otra en la que un tipo de evidencia entra en conflicto o se opone a otra. En este último caso, el conflicto debe resolverse: o bien una de las evidencias no se ha valorado correctamente, o los resultados han sido malinterpretados, lo que indica que no se ha ejercido un juicio profesional adecuado.

- b) Evidencia de auditoría** (en función de un determinado estándar): Se refiere a la “información utilizada por el auditor para alcanzar las conclusiones en las que basa su opinión. La evidencia de auditoría incluye tanto la información contenida en los registros contables de los que se obtienen los estados financieros, como otra información” (NIAS 500:2023).

De igual forma, la ISO 19.011:2018 define la evidencia objetiva como aquellos “datos que respaldan la existencia o veracidad de algo” (3.8) tales como: “registros, declaraciones de hechos u otra información relevante para los criterios de auditoría y que es verificable” (3.9).

Por otra parte, según la norma 14.1, la evidencia de auditoría se describe como la información utilizada por los auditores internos para llegar a conclusiones sobre su trabajo. Esta evidencia debe ser suficiente, relevante y confiable, y constituye la base sobre la cual se evalúan los hallazgos, conclusiones y recomendaciones en un trabajo de auditoría (NOGAI:2025).

En cuanto las auditorías efectuadas por la Contraloría General de la República, se define como Información empleada por el (la) auditor(a) para llegar a las conclusiones que sirven de fundamento a una opinión, un informe u otros productos de auditoría. La evidencia de auditoría incluye los antecedentes contenidos en sistemas informáticos, bases de datos, registros contables subyacentes a los estados financieros, entre otros (Resolución 10:2021, CGR).

- c) Evidencia digital:** Información o datos almacenados o transmitidos en forma binaria que se ha determinado mediante el proceso de análisis que son relevantes para una investigación (ISO 27.042:2015).

A su vez, la norma chilena la define como cualquier información en formato digital que puede ser usada en un proceso legal, y proporciona directrices para su análisis e interpretación. La norma establece que es fundamental asegurar la continuidad, validez, reproducibilidad y repetibilidad del análisis de la evidencia digital (NCh-ISO/IEC 27042:2019).

- d) Cadena de custodia:** Se define como el conjunto de procedimientos que permiten el seguimiento y control del estudio de la evidencia, con el fin de garantizar la integridad, identidad, preservación, seguridad y aptitud de los mismos a lo largo del proceso investigativo. Ellos hacen posible certificar que la evidencia es la misma desde su

obtención hasta su valoración en la etapa del juicio y que en los análisis se refleja, de la manera más precisa posible, lo ocurrido en el momento del hecho (Resolución Exenta 3363:2013, Servicio Médico Legal).

- e) **Criterios de auditoría:** conjunto de requisitos (3.23) usados como referencia frente a la cual se compara la evidencia objetiva (3.8) (ISO 19.011:2018). El ejemplo más representativo son las Normas de Auditoría.
- f) **Criterios de evaluación:** Como parte del trabajo de auditoría interna, las especificaciones del estado deseado de la actividad bajo revisión (NOGAI:2025).
- g) **Hallazgos de auditoría:** Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría (ISO 19.011:2018).
- h) **Hallazgo:** Como parte del trabajo de auditoría interna, la determinación de que existe una brecha entre los criterios de evaluación y la condición de la actividad bajo revisión. Se podrán emplear otras denominaciones como “observaciones” (NOGAI:2025).
- i) **Conclusiones de auditoría:** Es resultado de una auditoría (3.1), tras considerar los objetivos de la auditoría y todos los hallazgos de la auditoría (ISO 19.011:2018).
- j) **Conclusión del trabajo:** El juicio profesional de los auditores internos con respecto a los hallazgos del trabajo cuando se consideran de manera conjunta. La conclusión del trabajo debería indicar si el desempeño es satisfactorio o no satisfactorio. (NOGAI:2025).
- k) **Prueba legal:** Medio probatorio específico que la ley exige para acreditar un determinado hecho (DPEJ, 2024). En nuestro ordenamiento jurídico se ha regulado la prueba legal tanto en el Código de Procedimiento Civil como en Código Procesal Penal.
- l) **Prueba válida:** Prueba obtenida de forma lícita, esto es, sin vulnerar ningún derecho fundamental, y practicada con las garantías formales necesarias, en esencia, con posibilidad de contradicción e inmediatez (DPEJ, 2024).

IV. ACERCA DE LA “VERDAD” EN EL PROCESO DE AUDITORÍA

4.1. Los criterios de verdad

En este apartado, debemos comenzar haciéndonos la siguiente pregunta: ¿Cuándo puede un auditor tener certeza de que algo es “cierto” o “verdadero”? El destacado jurista en derecho contable, Mans Puigarnau, nos ofrece una explicación clara sobre este tema⁵. En este documento se extraen sus ideas sobre cómo se alcanza de manera natural la certeza

⁵ MANS PUIGARNAU, JAIME, 2015, “Lógica para Juristas”, Bosch Casa Editorial S.A., Barcelona, 1978, pág. 180-188, citado por HERNANDO BERMÚDEZ GÓMEZ, Parte II, Evidencia en Auditoría, “Auditoría y Control”, Pontificia Universidad Javeriana, Colombia.

del "conocimiento verdadero", explicadas de forma sencilla y accesible, sin necesidad de entrar en complejos ejercicios dogmáticos.

En tal sentido, Mans sostiene que existen medios naturales que nos proporcionan acceso al conocimiento, es decir, fuentes desde donde surge el "conocimiento cierto de la verdad".

Estas fuentes del conocimiento - que también influyen en la labor del auditor - incluyen: la experiencia o los sentidos externos, la experiencia interna, la conciencia o sentido íntimo, el sentido común natural, la evidencia intuitiva o discursiva, y la autoridad. Dicho de manera más resumida, las fuentes de conocimiento generalmente admitidas son la experiencia, la conciencia, el sentido común, la evidencia y la autoridad. En otras palabras, estas fuentes son los medios que utilizamos para alcanzar el "conocimiento cierto de una verdad" como se detallará más adelante en la sección sobre la "verdad" en auditoría. Consideradas objetivamente, estas fuentes constituyen el criterio "*per quod*" de la verdad, es decir, - según Mans - aquello mediante lo cual obtenemos el conocimiento cierto de una verdad.

Por otro lado, Mans también destaca la existencia del "criterio de la verdad", considerado subjetivamente como el llamado criterio "*secundum quod*", que se refiere a aquello según lo cual reconocemos certeramente algo como verdad a través de sus distintas fuentes, diversificándose en varias manifestaciones.

En este contexto, Mans clasifica estos "criterios de la verdad" de la siguiente manera:

a) Criterio de los sentidos o de la experiencia externa

Los sentidos externos, además de su función vital, proporcionan al entendimiento el conocimiento sensible con el cual se elaboran los conocimientos puramente intelectuales. El conocido axioma filosófico "*Nihil est in intellectu quod prius non fuerit in sensu*" cuya traducción es «nada hay en el entendimiento que antes no haya estado en los sentidos», expresa esta idea.

Sin embargo, el autor destaca que la verdad es que los sentidos pueden engañarnos, lo cual constituye el principal argumento de los escépticos. Pero también es verdad que esta posibilidad de error desaparecería si se cumplen ciertas condiciones que permiten evitar o corregir aberraciones. Bajo estas condiciones, la experiencia externa puede considerarse un criterio infalible de verdad, por lo que merecería plena confianza.

Las condiciones que, según este erudito, deben cumplirse son las siguientes:

1. Los sentidos deben estar en debida disposición y en estado normal, tanto en lo orgánico como en lo funcional, así como el sistema nervioso que transmite y recibe sus impresiones.
2. La relación entre el sentido y el objeto sensible debe establecerse de manera natural, eliminando posibles obstáculos. Si intervienen artificios, es necesario valorar previamente sus fines y efectos.
3. El sentido debe aplicarse al objeto con la debida atención, especialmente tratándose de los *sensibilia propria* (cualidades sensibles que solo pueden ser percibidas por un solo sentido, como el color, el sonido, el olor, el sabor, etc.) y considerando las

- impresiones de diversos sentidos cuando se trata de *sensibilia communia* (cualidades percibidas por dos o más sentidos, como la magnitud, el movimiento, la figura, etc.).
4. El testimonio de los sentidos debe ser constante y uniforme, sin contradicciones entre los datos proporcionados por diferentes sentidos.
 5. El entendimiento debe guiar su ejercicio y evaluar las percepciones obtenidas.

Impacto en el auditor: Para llevar este análisis a un contexto práctico, como se demostrará en este documento técnico, el criterio de los sentidos está estrechamente relacionado con la aplicación activa del juicio profesional. Este juicio es un atributo fundamental del debido cuidado profesional que el auditor debe ejercer.

b) Criterio de la conciencia o de la experiencia interna

La conciencia, también llamada "sentido íntimo", nos proporciona la experiencia interna, que consiste en el conocimiento inmediato no solo de nuestra propia existencia, sino también de nuestros actos psíquicos. En otras palabras, a través de la conciencia no solo observamos los actos mentales mediante los cuales conocemos algo, sino que también nos percatamos del propio sujeto que es el principio de esos actos. Dicho de manera sencilla, la conciencia es una función del entendimiento que nos permite no solo conocer las cosas, sino también darnos cuenta de que conocemos, y de que somos nosotros quienes conocemos. Así, por la conciencia, no solo nos enteramos de que conocemos, sino también de que sentimos y queremos, además de todos los actos propios de la vida psíquica sensible. En este sentido, la conciencia es, en última instancia, la intuición del "yo".

Mans continúa señalando que la conciencia perfecta es la conciencia refleja, es decir, el conocimiento que el alma tiene de sus propios actos y de su existencia mediante la reflexión. La "reflexión", nos dice, es el acto con el cual el alma vuelve sobre sus propias operaciones y sobre sí misma. El entendimiento, como fruto de su actividad, puede revisar y examinar retrospectivamente sus acciones (lo que hoy llamaríamos "retroalimentación" o *feedback*). Esta capacidad de reflexión es exclusiva del entendimiento y se aplica no solo a los actos cognitivos, sino a todas las funciones de nuestra vida psíquica. La conciencia o sentido íntimo sería, por tanto, un criterio infalible de verdad en lo que respecta a su objeto propio, que consiste en los actos de la vida psíquica, tanto sensitiva como espiritual, y en la existencia del "yo" como sujeto de esos actos. Esto es así porque no podría haber percepción sin un sujeto que perciba, ni conciencia sin un sujeto consciente, del mismo modo que no habría efecto sin causa. Sentir o percibir algo sin que lo percibido exista en la realidad sería inconcebible.

Impacto en el auditor: En este contexto, prevalece la aplicación activa del escepticismo profesional, cuyo Documento Técnico N° 128 contiene las bases para su comprensión y aplicación.

c) Criterio del sentido común (instinto intelectual)

El sentido común (*sensus naturae communis* o *common sense*, en latín) consistiría, según el autor, en una propensión innata del entendimiento a asentir a ciertas verdades o principios comunes a todos los seres humanos, incluso antes de que se manifiesten con

evidencia. Sería una especie de hábito intelectual que nos permite formular juicios casi instintivamente.

Por ejemplo, la humanidad reconoce verdades morales y distingue entre el bien y el mal, o principios y normas jurídicas fundamentales, como el hecho de que no se debe matar ni robar. Frecuentemente, se presentan cuestiones simples y elementales en nuestras conversaciones que descartamos automáticamente diciendo: "Esto es sentido común" o "Es lo más natural".

Sin embargo, el criterio del sentido común debe considerarse infalible solo si se cumplen las siguientes condiciones, que, según Mans, son las siguientes:

1. La verdad afirmada debe referirse a alguna necesidad elemental de la vida sensitiva, intelectual o moral.
2. La verdad debe contar con el ascenso universal de todos los hombres de todos los tiempos y lugares que estén en el uso normal de su razón.
3. La verdad debe poder someterse con éxito al examen de la razón.

Impacto en el auditor: El criterio del sentido común está estrechamente vinculado a la "regla del hombre prudente". Esta regla, a su vez, está relacionada con los estándares de auditoría sobre el "debido cuidado profesional", que se refiere al ejercicio del juicio con razonable inteligencia, competencias mínimas aceptables y basado en la experiencia.

Cabe recordar, que un proceso de auditoría no es un proceso abstracto, sino que es ejecutado por personas que combinan el sentido común, la experiencia y las observaciones en la aplicación de Normas de Auditoría (cualesquiera que sean o quienquiera que las emita), utilizando diversas técnicas. Por lo tanto, no puede existir un único método aplicable a todas las situaciones.

d) Criterio de la evidencia

El criterio de la evidencia nos lo proporciona directamente la razón, entendida en su sentido amplio como el entendimiento. Este incluye no solo la memoria, sino también la inteligencia, cuya función es la intuición, y la razón propiamente dicha, cuya función es el razonamiento argumentativo.

Mans señala que, gracias a la inteligencia, conocemos de manera inmediata las verdades universales que surgen de la comparación de ideas fundamentales organizadas entre sí. Estas verdades incluyen los *principia per se nota*, es decir, principios evidentes por sí mismos que no requieren ni admiten demostración. Uno de estos principios es el "principio de la evidencia", que se enuncia como "lo evidente es verdadero". Esto se traduce en la regla de que "la evidencia es un criterio certero de verdad". De ello se desprende que el principio que legitima la evidencia debe ser considerado evidente en sí mismo, ya que lo contrario nos llevaría al absurdo de negar la propia evidencia.

Mans también señala que, mientras la inteligencia, a través de la intuición, nos muestra la verdad de los principios evidentes por sí mismos, la razón, mediante el razonamiento deductivo o inductivo, convierte en evidentes aquellas verdades que no lo son por

naturaleza. Esto se logra comparándolas con verdades ya evidentes por sí mismas o "evidenciadas" a través de razonamientos previos.

En resumen, la inteligencia y la razón son las facultades que proporcionan al entendimiento las herramientas necesarias para adquirir la "evidencia de la verdad", ya sea de manera inmediata (intuitiva) o mediata (discursiva), dependiendo de la naturaleza de la verdad en cuestión. Así, la evidencia, siempre que se dé bajo condiciones de normalidad mental o "uso de razón", constituye un criterio infalible de verdad.

Impacto en el auditor: El auditor debe aplicar las reglas de la evidencia, ya sea porque los estándares lo exigen o porque los criterios que utiliza para establecer dicha evidencia lo demandan (proceso heurístico).

e) Criterio de autoridad

Mans señala que la palabra "autoridad" puede entenderse en dos sentidos: el primero, como el mando que ejerce una persona sobre sus subordinados, y que por lo misma le deben obediencia; segundo, la fe o crédito que, por derecho, merito o reputación se atribuye a una persona, y a la que por la misma se debe creencia. Es en este segundo sentido en el que habría que tomarla cuando se habla del "criterio de autoridad", el cual presupone que la persona investida de tal autoridad sea digna de creerse, o, en una palabra, que sea "fidedigna". Por lo tanto, la condición indispensable para que el criterio de autoridad sea infalible y pueda depositarse toda la confianza en él, es la credibilidad de la persona que da o presta la autoridad, la cual a su vez requiere la ciencia o conocimiento de la verdad, y la veracidad o intención de manifestarla.

La autoridad, basada en la credibilidad y esta a su vez en la ciencia y veracidad, da lugar a la fe o creencia. Esta se define como la admisión o aceptación de una verdad en función de haber sido manifestada y garantizada por una persona que goza de autoridad; o, según la definición tradicional: "*assensus, quo tenemus vera esse, quae dicuntur, propter auctoritatem dicentis*" (asenso por el cual tenemos como verdaderas las cosas que se dicen por razón de la autoridad del dicente).

Por otro lado, si la lógica está vinculada únicamente a la autoridad humana, debería observarse que esta puede garantizarnos tanto doctrinas (por ejemplo, verdades teóricas o prácticas cuya fuente de conocimiento es la razón) como hechos, es decir, fenómenos que caen bajo el dominio de la experiencia.

Por consiguiente, si hablamos de autoridad humana, Mans distingue entre dos tipos de testimonios:

1. Dogmático, que refiere a doctrinas o verdades teóricas o prácticas cuyo origen es la razón. En este caso, la autoridad humana no es la fuente directa del conocimiento ni el criterio adecuado de verdad, ya que ese papel corresponde a la razón y a la evidencia.

En resumen, el criterio de autoridad solo es aplicable cuando es necesario suplir la falta de conocimiento propio con el saber de personas dedicadas, profesionales o

expertas en un campo determinado. Mans agrega que, en el caso de una ciencia, el criterio de autoridad sería insuficiente sin los fundamentos correspondientes; en tal caso, el testimonio dogmático vale tanto como las razones que lo sustentan, según el aforismo: *In scientia tantum valet auctoritas quantum rationes* (en ciencia, la autoridad vale tanto como las razones que la fundamentan).

2. Histórico, que versa sobre hechos experimentados que no podemos percibir debido a limitaciones de tiempo o lugar. En este caso, la autoridad humana es la única fuente de conocimiento, y si se cumple el requisito de credibilidad, constituye un criterio certero de verdad (evidencia).

En el caso del testimonio histórico transmitido por tradición, para que este sea fidedigno, deben cumplirse tres condiciones:

- Que el hecho relatado sea público y notorio (*factum sit publicum et illustre*).
- Que la transmisión del hecho sea continua, es decir, ininterrumpida (*traditio sit perpetua*).
- Que la noticia se haya propagado en un ámbito amplio (*traditio sit ampla*).

Ahora, si el relato se transmite por documentos, para que prueben el hecho a que se refieren estos deben cumplir con requisitos como: autenticidad (ser obra del autor y de la época correspondiente), integridad (sin alteraciones, modificaciones, añadidos o interpolados), y en caso de alteraciones, debe buscarse restituir el texto a su estado original.

Por ejemplo, en la prueba testimonial, la ley adopta precauciones para garantizar la credibilidad de los testigos, siendo crucial que las tachas de éstos se basen en motivos que anulan o restan valor, afectando dicha credibilidad, la cual será valorada por el juez según su criterio. De manera similar, un auditor debe considerar estas precauciones al evaluar los testimonios del auditado.

En cuanto a los documentos, la ley establece garantías necesarias y suficientes para verificar su autenticidad, valorando incluso su antigüedad al fundar en ella como presunción de su pureza original, lo que puede eximir en algunos casos el cotejo con originales y matrices.

Impacto en el auditor: El criterio de autoridad está estrechamente vinculado a los tipos de evidencia de auditoría, como las "entrevistas de indagación", donde el auditor debe profundizar en los dichos del auditado. En el acápite siguiente 5.4. se aborda en detalle esta materia.

En tal sentido, las Normas Globales de Auditoría Interna establecen que los auditores deben evaluar críticamente la información proporcionada por la actividad bajo revisión, aplicando escepticismo y cuidado debido profesional. Esto implica identificar posibles inconsistencias o señales de fraude, sin sustituir la necesidad de consultar a expertos externos en autenticación cuando sea necesario. Por lo tanto, el auditor debe centrarse

en verificar la coherencia y validez de los documentos mediante procedimientos de auditoría adecuados, apoyándose en especialistas en casos que requieran una evaluación técnica más detallada.

De igual forma, en el contexto de las Normas de Auditoría Externa, no se espera que el auditor sea un experto en autenticación documental; para ello, debe recurrirse a un especialista.

4.2. El camino hacia “la verdad” en un proceso de auditoría

Como se mencionó previamente, y complementando lo expuesto por Mans, la evidencia proporciona los medios para alcanzar ese estado de seguridad que llamamos “saber”, en lugar de simplemente “creer”. La clave de la “verdad”, en el contexto de la Auditoría, puede describirse como “conformidad con la realidad”. Como auditores, nos esforzamos por alcanzar cierto grado de verdad mediante el uso de nuestros sentidos, pero este camino no siempre resulta confiable.

Antes de avanzar, es necesario comprender en pocas palabras qué es la “verdad”. Esta, de acuerdo con Mautz y Sharaf, se puede dividir en tres tipos, complementándose con el trabajo de Mans:

1. Verdades materiales
2. Verdades matemáticas
3. Verdades abstractas

Esta clasificación será útil al abordar el problema de la verificación del auditor y los medios para obtenerla. A continuación, se presentan las principales posturas de estos autores, precisando algunas cuestiones relacionadas con el rol del auditor, como complemento de las ideas base propuestas por ellos.

Ellos indican que las “verdades materiales” son aquellas que quedan grabadas en nuestra mente mediante la evidencia natural. Escoto -citado por Mautz y Sharaf- describe que la mente tiene cualidades que la obligan a aprehender objetos y acontecimientos llevados a la atención inmediata de los sentidos. De esta manera, la mente no puede negar haber visto un objeto colocado frente a nuestros ojos (suponiendo que funciona normalmente), por lo que está “obligada” a asentir ante la existencia de lo que se le manifiesta. Así, si tenemos un objeto que existe naturalmente (es decir, cuya propia evidencia confirma su existencia) y que puede percibirse clara y distintamente, la mente necesariamente lo aprehende y acepta su existencia. Cuando esto ocurre, la mente adquiere una certeza de conocimiento; no solo sabe, sino que sabe que sabe, y no hay lugar para la duda.

Algunos eruditos pueden cuestionar si alguna vez será posible alcanzar una certeza absoluta, pero ese es un argumento demasiado técnico para los fines de un auditor. Es útil, sin embargo, estar conscientes de este concepto de certeza para compararlo luego con la seguridad que se tiene respecto a otros tipos de verdad.

Por otro lado, las “verdades matemáticas” son aquellas que derivan de la aceptación de los postulados y supuestos básicos de las matemáticas. Aceptamos como cierto que dos más dos son cuatro sin considerar (ni cuestionar) que esto se basa en ciertos supuestos

sobre la naturaleza de la unidad, los significados de los términos involucrados y las reglas para la manipulación de los números. En efecto, las matemáticas tratan con abstracciones, y cualquier número es una abstracción. Las verdades abstractas de tipo matemático serán lo suficientemente simples mientras las comprendamos. Sabemos con tanta certeza que dos más dos son cuatro como sabemos que la mesa que tenemos frente a nosotros existe.

Finalmente, las “verdades abstractas” ofrecen una gran diversidad y distintos grados de complejidad. Sabemos, por ejemplo, que la Tierra gira alrededor del Sol; es decir, aceptamos esto como un hecho cierto. Pero ¿nuestra mente está tan segura de esta proposición como lo está respecto a la existencia de una mesa o de que dos más dos son cuatro? Por su naturaleza, las verdades abstractas y no matemáticas resultan más difíciles de comprender y aceptar para algunas personas.

Para comprender las verdades abstractas y no matemáticas, se requiere argumentación racional. En este caso, la mente debe inferir la verdad de una proposición a partir de una combinación de evidencias. Por ejemplo, es posible que un amigo haya visto el Edificio Costanera y testifique sobre su existencia. La mente razona que este amigo es una persona honesta, que no tiene motivo para engañar, que es capaz de reconocer un objeto de esa descripción, y por lo tanto, puede aceptarse su testimonio. Mientras que la mente se ve obligada a aceptar lo que percibe directamente, no está obligada a aceptar lo que aprehende indirectamente. La mente puede ser fuertemente persuadida, pero no está forzada a aceptarlo. A esto se enfrentan frecuentemente los auditores: lo razonable y lo tolerable dentro de un conjunto de evidencias.

Recordemos que las Normas Globales de Auditoría Interna señalan que los auditores internos realizan evaluaciones objetivas para proporcionar aseguramiento. Agregando que podrán proporcionar aseguramiento limitado o razonable, dependiendo de la naturaleza, el momento o la extensión de los procedimientos ejecutados.

Por su parte, la Sección AU 200.5 de las normas internacionales de auditoría indican *“La seguridad razonable no es de un nivel absoluto de seguridad debido a que existen limitaciones inherentes en una auditoría que resultan en que la mayor parte de la evidencia de auditoría, sobre la cual el auditor llega a conclusiones y basa la opinión del auditor, sea más bien persuasiva en vez de concluyente”*. Esto no es muy diferente de lo que concluye un auditor interno.

Obviamente, no se podría avanzar mucho en cualquier campo de estudio que se limite a las verdades materiales o incluso a las verdades matemáticas y materiales. Debemos ir más allá de la mera comprensión y descripción. No es una novedad que cada disciplina incluye muchas “verdades abstractas” (por ejemplo, el Marco Conceptual de la Información Financiera). Debe reconocerse que estas verdades son diferentes de las naturales y matemáticas, y requieren distintos tipos de evidencia para ser aceptadas.

La certeza absoluta sobre las proposiciones abstractas es un imposible, pero pueden ser tan altamente probables que se acerquen a la certeza. Sin embargo, si la evidencia no es sólida, la mente puede resistirse a aceptar el razonamiento y podríamos estar ligeramente más inclinados a aceptar la proposición como verdadera que a considerarla falsa.

En el ámbito de la auditoría, encontramos diferencias adicionales en la naturaleza de los problemas y en la evidencia en la que se basa. La auditoría se ocupa de la protección de quienes leen, por ejemplo, los estados financieros. Su propósito es asegurarles que se han cumplido ciertos estándares de precisión, claridad e integridad, pero no de manera absoluta.

Debemos comprender que el quehacer de la auditoría probablemente es más limitado que el de otros campos del saber, pero sus problemas específicos no son necesariamente más limitados que los de otras áreas del conocimiento. El tema central de la evidencia de auditoría radica en las proposiciones contenidas en los objetos de análisis (por ejemplo, estados financieros u otros datos financieros). Parte de esta evidencia se obtiene mediante “dones”, por así decirlo; otra se busca o crea por el auditor, y otra se infiere a partir de otras evidencias (indicios). Lo cierto es que un auditor recibe cierta información de los empleados y directivos de la entidad auditada, y a partir de allí desarrolla otros datos enviando confirmaciones, preparando conciliaciones y análisis, y realizando pruebas adicionales que derivan de su propia línea de razonamiento, comparando el presente caso con otros similares de su experiencia. Así, el auditor, quien emite juicios, asume principalmente un papel activo en el desarrollo de la evidencia, aunque en algunos casos recibe ciertos tipos de evidencia de manera pasiva.

Como mencionamos en el Documento Técnico N° 127 sobre el escepticismo profesional, el tiempo es un recurso crucial en la mayoría de los trabajos de auditoría. El juicio del auditor normalmente se requiere en un plazo relativamente corto. A su vez, el tiempo es vital en otro sentido, especialmente si el control interno no es tan robusto como se desearía. Por consiguiente, el tiempo es esencial tanto para la recopilación de evidencia de auditoría como para la formación de juicios.

En conclusión, la evidencia de auditoría influirá en el auditor en grados que varían desde lo completamente convincente hasta lo meramente persuasivo. Un ejemplo de lo primero es cuando se ha visto y contado la caja chica; el auditor se ve obligado a aceptar su existencia y su importe. Un ejemplo de lo segundo es la “calidad” de la cobrabilidad de las cuentas por cobrar, donde el auditor puede estar convencido de que, en general, son cobrables, pero raramente puede estar absolutamente seguro de ello.

V. CARACTERÍSTICAS, TIPOLOGÍA Y LIMITANTES DE LA EVIDENCIA EN LA LABOR DEL AUDITOR⁶

5.1. Naturaleza de la evidencia en auditoría

Como hemos mencionado a lo largo de este documento, el uso de la evidencia no es exclusivo de los auditores. La evidencia también es ampliamente utilizada por científicos, abogados, médicos, psicólogos, periodistas, arqueólogos, historiadores, entre otros. Por ejemplo, en los casos legales, como veremos más adelante, existen reglas bien definidas sobre la evidencia que los jueces aplican en los procesos judiciales, las cuales se

⁶ Algunas ideas y explicaciones metodológicas se han tomado, adaptadas y resumidas del Bestseller “Auditing and Assurance Services: An Integrated Approach”, Sixteenth Edition, Global version, ALVIN A. ARENS (†), RANDAL J. ELDER, MARK S. BEASLEY AND CHRIS E. HOGAN, Pearson Education, 2017.

relacionan con la admisibilidad de las piezas de prueba. Otro ejemplo son los experimentos científicos, en los que los investigadores obtienen evidencia para probar hipótesis mediante experimentos controlados, como los ensayos clínicos para probar la efectividad de un nuevo tratamiento médico. En este contexto, la recopilación de evidencia es una parte fundamental del trabajo de los auditores.

De hecho, al revisar las Normas Globales de Auditoría Interna, encontramos que la palabra "evidencia" se menciona 89 veces (incluyendo la evidencia de conformidad) en un documento de 120 páginas, con una frecuencia de una vez cada 0.7 páginas. Esto refleja su importancia para sustentar hallazgos, asegurar objetividad y demostrar conformidad, siendo esencial en todas las etapas del proceso de auditoría, garantizando transparencia y calidad en los resultados.

Del mismo modo, si revisamos las Normas de Auditoría Externa, encontramos que la palabra "evidencia" aparece 1,421 veces en un manual de 879 páginas, lo que significa una frecuencia de aparición cada 0.6 páginas, subrayando también su relevancia en labor del auditor.

En resumen, tanto abogados, científicos como auditores, se basan en diferentes tipos de evidencia y la usan en diferentes entornos, de diferentes maneras, con el único objetivo de ayudarlos a sacar sus conclusiones.

Para el auditor, la evidencia es el eje central de su trabajo. No existe procedimiento ni técnica de auditoría en la que la evidencia no esté presente. La evidencia (o la información, según corresponda) sirve para diseñar y aplicar procedimientos de auditoría adecuados, teniendo en cuenta las circunstancias, con el fin de obtener una evidencia: suficiente, pertinente, fiable, oportuna y relevante.

Dado que la evidencia es crucial para el trabajo del auditor, las Normas de Auditoría, cualesquiera que sean éstas, exigen que la evidencia cumpla con ciertos estándares mínimos de calidad. El auditor solo puede concluir si ha obtenido "evidencia de auditoría relevante, fiable y suficiente". Por lo tanto, la determinación de si se ha obtenido evidencia con tales características (para reducir el riesgo de auditoría a un nivel aceptablemente bajo y llegar a conclusiones razonables) también requiere juicio profesional, que puede implicar factores como la naturaleza de los procedimientos de auditoría, la oportunidad de la información que recibe el auditor y la relación costo-beneficio en la toma de decisiones.

5.2. Características de la evidencia en auditoría

En general, las normas de auditoría requieren que el auditor acumule suficiente evidencia apropiada para respaldar su opinión. Debido a la naturaleza de la evidencia de auditoría y a las consideraciones de costo-beneficio de realizar una auditoría, es poco probable que el auditor esté completamente convencido de que la opinión es correcta. Sin embargo, el auditor debe estar persuadido de que la opinión es correcta con un alto nivel de seguridad. Al combinar toda la evidencia de la auditoría, el auditor puede decidir cuándo se le persuade para emitir un informe de auditoría. La literatura técnica reconoce dos determinantes clave para la capacidad de persuasión de la evidencia: idoneidad (también llamada adecuación) y suficiencia. Aunque la palabra "idoneidad" no se menciona

explícitamente en las Normas Globales de Auditoría Interna (NOGAI), su esencia se encuentra implícita en el análisis de la calidad global de la evidencia recopilada por los auditores internos. Este concepto integra la relevancia y la fiabilidad, es decir, que la evidencia sea pertinente para los objetivos de la auditoría y provenga de una fuente confiable, permitiendo sustentar adecuadamente los hallazgos y conclusiones.

En este contexto, la idoneidad de la evidencia se refiere a una medida de su calidad (aspecto cualitativo), es decir, su relevancia y fiabilidad para cumplir con los objetivos de auditoría relacionados con clases de transacciones, saldos de cuentas y revelaciones. Cuando la evidencia es altamente apropiada, facilita persuadir al auditor de que el objeto auditado está adecuadamente fundamentado.

Es importante recordar que la idoneidad se refiere solo a los procedimientos de auditoría seleccionados. De ahí que la idoneidad no se puede mejorar seleccionando un tamaño de muestra más grande o sobre diferentes elementos de la población de estudio. En cambio, sí podría mejorarse mediante la selección de procedimientos de auditoría más pertinentes o que proporcionen una evidencia más fiable.

La primera cualidad de la evidencia es que debe ser relevante para el objetivo de auditoría que se persigue antes de que se le califique de apropiada. Por ejemplo, supongamos que al auditor le preocupa que un cliente no esté facturando a los clientes por los envíos (objetivo de la transacción de integridad). Si el auditor selecciona una muestra de facturas de venta y rastrea cada una de ellas hasta los documentos de embarque relacionados, la evidencia no es relevante para el objetivo de integridad y, por lo tanto, no es evidencia apropiada para ese objetivo. Un procedimiento relevante sería rastrear una muestra de documentos de envío hasta las facturas de venta para determinar si se facturó cada envío. Este segundo procedimiento es relevante porque el envío de mercancías es el criterio habitual para determinar si se ha producido una venta y si se debería haber facturado. Al rastrear desde los documentos fuentes de envío hasta las facturas de venta, el auditor puede determinar si los envíos se han facturado a los clientes. En el primer procedimiento, en cambio, cuando el auditor rastrea desde facturas de venta hasta los documentos de envío, es imposible encontrar envíos no facturados.

En consecuencia, la relevancia solo puede considerarse en términos de los objetivos de auditoría específicos, ya que lo que puede ser pertinente para un objetivo de auditoría no necesariamente lo es para otro.

La segunda cualidad de la evidencia es su fiabilidad, que hace referencia al grado en que la evidencia puede ser creíble o digna de confianza. Al igual que la relevancia, si la evidencia se considera confiable, es de gran ayuda para persuadir al auditor de que el objeto a examinar está bien definido. Por ejemplo, si un auditor cuenta el inventario, esa evidencia es más confiable que si la actividad bajo revisión le da al auditor sus propios montos del recuento.

La relevancia y fiabilidad, es decir, la idoneidad, dependen de las siguientes seis características de la evidencia:

- a) Independencia del proveedor:** La evidencia obtenida de una fuente externa a la actividad bajo revisión es más confiable que la obtenida internamente. Las comunicaciones de bancos, abogados o clientes generalmente se consideran más confiables que las respuestas obtenidas de las consultas del cliente. Del mismo modo, los documentos que se originan fuera de la organización, como una póliza de seguro, se consideran más confiables que los documentos originados dentro del servicio, como una orden de compra que nunca ha salido de la institución.

Recomendación: Procure acceder a información externa que le permita confirmar los objetivos establecidos, para reducir los tiempos de revisión y canalizar de mejor manera los recursos asignados a los distintos procesos de auditoría.

- b) Efectividad de los controles internos de la actividad bajo revisión:** Cuando los controles internos de la actividad bajo revisión son efectivos, la evidencia obtenida es más confiable que cuando no lo son. Por ejemplo, si los controles internos sobre las ventas y la facturación son idóneos, permitirán que el auditor obtenga evidencia más confiable que en un entorno donde los controles no existen o son inadecuados.

Recomendación: Cuando el auditor interno colabora directamente en la efectividad de los controles internos, puede transformarse en “juez y parte” sobre la efectividad de esos controles, afectando su objetividad e independencia. Para minimizar este riesgo, es importante establecer controles de calidad como la oposición de controles, rotación de auditores y una política permanente de compromiso con la auditoría desde la gobernanza.

- c) Conocimiento directo del auditor:** La evidencia obtenida directamente por el auditor a través del examen físico, la observación, el recálculo y la inspección es más confiable que la información obtenida indirectamente. Por ejemplo, si el auditor calcula el margen bruto como un porcentaje de las ventas y lo compara con períodos anteriores, la evidencia es más confiable que si se basa en cálculos proporcionados por la actividad bajo revisión.

Recomendación: En determinados casos, la evidencia indirecta puede ser útil cuando no existe en las dependencias de la actividad bajo revisión, especialmente cuando se detectan irregularidades que comprometen la función pública y el uso correcto de los recursos públicos.

- d) Cualificaciones de las personas que proporcionan la información:** Aunque la fuente de información sea independiente, la evidencia no será confiable a menos que la persona que la proporcione esté calificada para hacerlo. Por lo tanto, las comunicaciones de abogados y confirmaciones bancarias, por ejemplo, suelen ser más valoradas que las confirmaciones de cuentas por cobrar proporcionadas por personas sin familiaridad con el mundo de los negocios. Además, la evidencia obtenida directamente por el auditor puede no siempre ser confiable si este carece de las cualificaciones necesarias para evaluar la evidencia. Por ejemplo, el examen de un inventario de diamantes realizado por un auditor no capacitado para distinguir entre diamantes y zirconia cúbica no es una “prueba fiable” de la existencia de diamantes.

Recomendación: El auditor interno debe asegurarse no solo de las cualificaciones de las personas que proporcionan la información, sino también de que dichas personas estén reconocidas institucionalmente para proveerla. Una primera verificación sería examinar los poderes legales que ostentan, como poderes notariales tradicionales, decretos o resoluciones administrativas.

- e) Grado de objetividad:** La evidencia objetiva (material formal) tiende a ser más confiable que aquella evidencia donde se requiere un juicio considerable por parte del auditor para determinar su idoneidad. Ejemplos de pruebas objetivas son la confirmación de cuentas por cobrar y saldos bancarios, el recuento físico de valores y efectivo, y la adición de una lista de cuentas por pagar para verificar si concuerda con el saldo del libro mayor. En cambio, ejemplos de evidencia subjetiva incluyen una carta de un abogado de la institución discutiendo el resultado probable de demandas pendientes, la observación de la obsolescencia del inventario durante el examen físico, y la declaración del encargado de créditos sobre la cobrabilidad de cuentas por cobrar.

Recomendación: Existen exigencias mínimas formales para la evidencia objetiva que un auditor debe siempre considerar, y que muchas veces se pasan por alto debido a la relación prolongada entre auditor y la actividad bajo revisión. Por ejemplo, es fundamental conocer qué documentos deben emitirse con Firma Electrónica Avanzada (FEA) en la administración pública y cuándo es obligatorio su uso. Algunos documentos administrativos, como email, cartas o memorándums, requieren solo Firma Electrónica Simple (FES), mientras que otros, como documentos electrónicos con la calidad de instrumento público (por ejemplo, una escritura pública o un certificado del Registro Civil), sí requieren FEA.

- f) Puntualidad:** La puntualidad de la evidencia de auditoría puede referirse tanto al momento en que se acumula como al período cubierto por la auditoría. La evidencia suele ser más confiable cuando se obtiene en el momento oportuno. Por ejemplo, el recuento de valores negociables realizado por el auditor sería más confiable que un recuento realizado meses antes, debido a la volatilidad de estos instrumentos. Esto hace que no se deba confiar en evidencia que ya no es pertinente al momento del análisis.

Recomendación: No se debe confundir la "impuntualidad" de la evidencia con la "extemporaneidad". Una evidencia puede adquirirse de manera oportuna, pero su contenido puede estar fuera del umbral temporal de análisis. Esto sucede, por ejemplo, con algunas certificaciones notariales de hechos muy anteriores a la auditoría. El hecho de que un notario emita una copia actualizada de un documento no significa que lo señalado en ese documento sea válido en el momento en que el auditor realiza su examen. Las formas no deben confundirnos.

Finalmente, la segunda determinante de la capacidad de persuasión de la evidencia es la suficiencia, que se refiere a la cantidad de evidencia.

Para algunos objetivos de auditoría, la suficiencia de la evidencia se mide principalmente por el tamaño de la muestra seleccionada. Para un procedimiento de auditoría dado, la evidencia obtenida de una muestra de 100 es normalmente más suficiente que la obtenida

de una muestra de 50. Para otros objetivos, la suficiencia está determinada por el número y la calidad de los procedimientos realizados para cumplir el objetivo de auditoría.

Son varios los factores que determinan el tamaño adecuado de una muestra de auditoría. Los dos más importantes son la expectativa del auditor de encontrar errores y la efectividad de los controles internos de la actividad bajo revisión. Por ejemplo, si el auditor concluye que existe una alta probabilidad de inventario obsoleto debido a la naturaleza de los productos (por ejemplo, computadores portátiles entregados en el marco de algún programa que buque acortar la brecha de acceso y uso de las tecnologías), tomará muestras de más artículos del inventario para determinar su obsolescencia, en comparación con una situación donde la probabilidad de obsolescencia sea baja. Por otro lado, si el auditor concluye que la actividad bajo revisión ha implementado adecuadamente sus controles internos, podría estar justificado un tamaño de muestra más pequeño respecto al stock disponible de esos computadores.

Además del tamaño de la muestra, los elementos individuales analizados afectan la suficiencia de la evidencia. En general, se consideran suficientes las muestras que contienen elementos de la población con grandes valores monetarios y que son representativas de la población. Por el contrario, la mayoría de los auditores consideran insuficientes las muestras basadas solo en atributos de importancia numérica. Aquí, el juicio profesional es crucial.

Por consiguiente, la capacidad de persuasión de la evidencia solo puede evaluarse después de considerar la combinación de idoneidad y suficiencia, incluidos los efectos de los factores que influyen en ello. Una muestra amplia de evidencia proporcionada por una fuente independiente no es persuasiva a menos que sea pertinente para el objetivo de auditoría que la motiva. Del mismo modo, una gran muestra de evidencia relevante, pero no objetiva, tampoco es persuasiva. Asimismo, una pequeña muestra de una o dos piezas de evidencia altamente apropiada también suele carecer de capacidad persuasiva. Al evaluar la capacidad de persuasión de la evidencia, el auditor debe considerar el grado en que se cumplen tanto la idoneidad como la suficiencia, incluidos todos los factores que influyen en ellas.

En resumen, al tomar decisiones sobre la evidencia en una auditoría, es esencial equilibrar la capacidad de persuasión de la evidencia y el costo asociado a su obtención. Rara vez se dispone de un único tipo de evidencia para verificar la información, por lo que antes de seleccionar el tipo o tipos de evidencia, se deben ponderar tanto su capacidad de persuasión como el costo de las alternativas disponibles. El objetivo del auditor es obtener una cantidad suficiente de evidencia apropiada al menor costo total posible, sin comprometer la calidad del trabajo. Sin embargo, el costo nunca debe ser una justificación para omitir procedimientos necesarios o reducir el tamaño de la muestra por debajo de lo adecuado. Un malentendido sobre la relación entre los riesgos y el ahorro de costos puede afectar negativamente la calidad de la auditoría.

5.3. Decisiones sobre la evidencia de auditoría

Una de las decisiones clave que debe tomar el auditor interno es determinar los tipos y la cantidad adecuada de evidencia que se debe recopilar para asegurarse de que los componentes de los informes financieros y presupuestarios de la actividad bajo revisión, así como los informes en su totalidad, se presenten con objetividad, o bien, que la actividad bajo revisión mantuvo un control interno efectivo sobre sus procesos administrativos y financieros. Este criterio es crucial debido al elevado costo que implicaría examinar y evaluar toda la evidencia disponible. Por ejemplo, en la auditoría de una actividad, es impracticable que el auditor revise todas las compras públicas, facturas de proveedores, solicitudes de servicio, registros electrónicos de asistencia para la nómina, entre otros documentos y registros.

Las decisiones del auditor respecto a la recolección de evidencia pueden clasificarse en las siguientes cuatro subdecisiones:

1. Cuáles procedimientos de auditoría aplicar.
2. Qué tamaño de muestra seleccionar para un procedimiento determinado.
3. Qué elementos de la población examinar.
4. Cuando realizar los procedimientos.

Un procedimiento de auditoría es la instrucción detallada para la obtención de un tipo específico de evidencia en un momento particular durante la auditoría. Al diseñar estos procedimientos, es común redactarlos de manera específica para que puedan ser utilizados como instrucciones claras durante el proceso. Por ejemplo, un procedimiento para la revisión de compras públicas podría ser el siguiente:

- Obtener el registro de compras públicas y comparar el proveedor, el monto y la fecha de la compra con la información registrada en los sistemas financieros de la actividad bajo revisión, verificando que los pagos se hayan realizado dentro del plazo de 30 días.

Una vez definido el procedimiento de auditoría, el tamaño de la muestra puede variar desde examinar una sola partida hasta todas las partidas de la población en cuestión. En el ejemplo anterior, si el registro de compras públicas contiene 3.300 transacciones, el auditor podría seleccionar una muestra de 25 compras para compararlas con el registro. La decisión sobre cuántas partidas examinar debe ser tomada por el auditor para cada procedimiento, y el tamaño de la muestra puede variar entre auditorías.

Después de determinar el tamaño de la muestra, el auditor debe decidir qué elementos de la población examinar. Por ejemplo, si se seleccionan 25 compras de una población de 3.300, se pueden utilizar varios métodos para escoger las transacciones a revisar: 1) examinar las primeras 25 compras de un periodo específico, 2) seleccionar las 25 compras de mayor monto, 3) escoger compras al azar, o 4) seleccionar aquellas que, según el auditor, tienen mayor probabilidad de presentar errores. También puede emplearse una combinación de estos métodos.

Las auditorías internas generalmente abarcan un período fiscal de un año, y rara vez se concluyen hasta varias semanas o meses después del cierre del ejercicio. Por lo tanto, los

procedimientos de auditoría pueden extenderse desde el inicio del período contable hasta tiempo después de su cierre. La duración de estos procedimientos depende, en parte, de la necesidad de la actividad bajo revisión de que la auditoría concluya. Las auditorías internas a menudo están alineadas con plazos legales o normativos, como los tiempos establecidos por los órganos de control. Además, otros factores, como la disponibilidad del equipo auditor o el momento en que la evidencia sea más efectiva, también influyen en la duración de los procedimientos. Por ejemplo, los auditores internos suelen preferir realizar la revisión de las compras públicas lo más cerca posible de la fecha de cierre del ejercicio fiscal, verificando también que los pagos a proveedores se realicen dentro del plazo establecido de 30 días.

Los procedimientos de auditoría frecuentemente incluyen consideraciones sobre el tamaño de la muestra, las partidas a seleccionar y la duración. A continuación, se presenta una modificación del procedimiento de revisión de compras públicas que incluye las cuatro decisiones sobre la evidencia de auditoría (las palabras en cursiva indican duración, selección de partidas y decisiones sobre el tamaño de la muestra):

- Obtener el registro de compras públicas de octubre y comparar el proveedor, el monto y la fecha de la compra con el registro de compras para una muestra aleatoria de 20 transacciones, verificando que el pago a proveedores se haya realizado dentro de los 30 días establecidos.

El conjunto de procedimientos de auditoría para un área específica o una auditoría completa recibe el nombre de programa de auditoría. Este programa siempre incluye una lista de procedimientos a seguir.

En algunos casos, los auditores internos utilizan herramientas tecnológicas para facilitar la preparación y ejecución de los programas de auditoría. Entre estas herramientas, se puede incluir el uso de planillas Excel para el análisis de grandes volúmenes de datos, técnicas de auditoría asistidas por computador (CAATs, por sus siglas en inglés), o software especializado de auditoría, que permiten realizar pruebas automatizadas. Actualmente algunos auditores pueden optar por utilizar herramientas basadas en inteligencia artificial para identificar patrones o detectar anomalías en los datos financieros. Estos enfoques pueden ayudar a mejorar la planificación, seleccionar muestras más precisas e identificar riesgos de manera más efectiva, incrementando así la calidad de la auditoría.

5.4. Tipos de evidencia en auditoría

En auditoría interna, la evidencia es fundamental para respaldar los hallazgos, conclusiones y recomendaciones de los auditores. La evidencia puede clasificarse en diferentes tipos o categorías según su naturaleza y fuente.

En el desarrollo de la auditoría, los procedimientos, técnicas y herramientas utilizadas, se documentarán en papeles de trabajo, que son la evidencia de la actividad realizada por los auditores, y que sustentan las conclusiones y hallazgos detectados en la auditoría.

Los procedimientos con respecto a la recopilación de información para su análisis podrán incluir: evidencia documental, física, testimonial, analítica, electrónica o digital, observacional, comparativa, entre otros.

Ahora, como se mencionó anteriormente, cuando se recopila información, los auditores internos consideran si realizarán pruebas sobre una población completa de datos o sobre una muestra representativa. El empleo de software de análisis de datos facilita la capacidad de probar poblaciones de datos completas o específicas. Si deciden seleccionar una muestra, deberían aplicar métodos para asegurar que la muestra sea lo más representativa posible de la población completa.

La oportunidad de dichos procedimientos dependerá, en parte, de los períodos de tiempo durante los que la evidencia de auditoría buscada esté disponible.

Al decidir qué procedimientos de auditoría se van a utilizar, el auditor puede elegir entre ocho amplias y comunes categorías de evidencia, que se denominan tipos de evidencia.

Antes de iniciar el estudio de los tipos de evidencias, es útil mostrar las relaciones entre las normas de auditoría, los tipos de evidencias y las cuatro decisiones de evidencias que se abordaron anteriormente. Estas relaciones se muestran en la figura 1.

Observe que las normas de auditoría son generales, en tanto que los procedimientos de auditoría son específicos. Los tipos de evidencia son más amplios que los procedimientos y más reducidos que las normas. Con cada procedimiento de auditoría se obtiene uno o más tipos de evidencias.

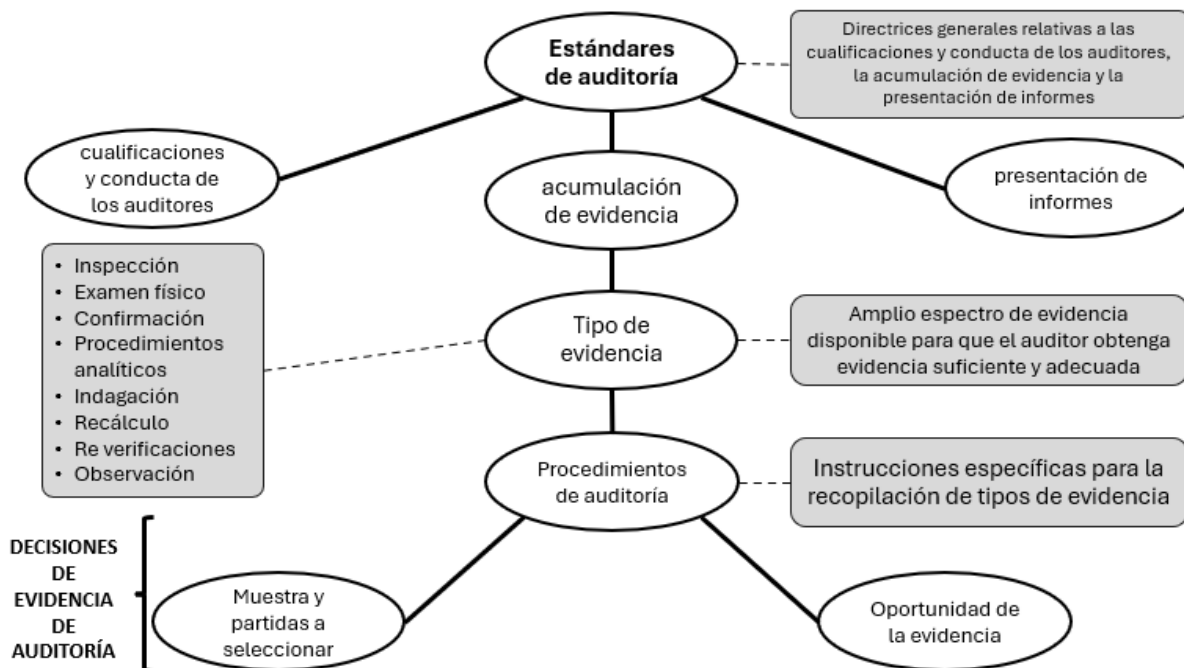


Figura 1: Relaciones entre normas de auditoría, tipos de evidencias y las decisiones sobre evidencias en auditoría
Fuente: Alvin A. Arens (†) et al, 2017

Ahora, todo procedimiento de auditoría nos permite obtener uno o más de los siguientes tipos de evidencia:

- 1. La inspección:** Es el examen, por parte del auditor, de los documentos y registros de la actividad bajo revisión para corroborar la información que está o debería incluirse en un determinado registro oficial. Los documentos examinados por el auditor son los registros utilizados por la actividad bajo revisión para proporcionar información y llevar a cabo sus actividades de manera organizada. Estos documentos pueden estar en papel, formato electrónico u otros medios. Dado que cada operación en la actividad bajo revisión normalmente está respaldada por al menos un documento, generalmente se dispone de un gran volumen de este tipo de evidencia. La documentación se utiliza ampliamente como evidencia en las auditorías porque suele estar fácilmente disponible a un costo relativamente bajo. A veces, es el único tipo razonable de evidencia disponible.

A continuación, los documentos se pueden clasificar convenientemente en internos y externos. El primero se refiere a un documento preparado y utilizado dentro de la actividad bajo revisión, el cual se conserva sin recurrir a una parte externa. Ejemplos concretos serían las resoluciones administrativas, informes de pagos de horas extras, informes de recepción de inventario, y comprobantes contables.

Por otro lado, un documento externo ha sido manejado por una parte ajena a la actividad bajo revisión, aunque esté actualmente en su poder o sea fácilmente accesible. Algunos ejemplos de documentos externos serían las facturas de los proveedores, las boletas de honorarios electrónicas, las pólizas de seguro, y cartolas bancarias.

El principal factor que determina si el auditor acepta un documento como evidencia confiable es si es interno o externo, y en caso de ser interno, si fue creado y procesado bajo condiciones de control interno efectivo. Los documentos internos creados y procesados en condiciones de control interno deficiente pueden no constituir una evidencia fiable (por ejemplo, un documento sin FEA que exigía cumplir con esa condición).

Debido a que los documentos externos han estado en manos tanto de la actividad bajo revisión como de un tercero ajeno a la operación, esto indica que ambas partes están de acuerdo sobre la información y las condiciones establecidas en el documento. Por lo tanto, los documentos externos se consideran evidencia más fiable que los internos. Algunos documentos externos, como los títulos de propiedad, las pólizas de seguro y los acuerdos contractuales, tienen una fiabilidad excepcional porque intervienen otros profesionales calificados (por ejemplo, abogados, notarios, etc.).

Generalmente, los auditores utilizan la documentación para respaldar las transacciones o los montos registrados, proceso que suele denominarse “verificación”. Para dar fe de las operaciones de adquisición registradas, el auditor podría, por ejemplo, verificar los asientos en el diario de adquisiciones examinando las facturas de los proveedores y/o recurriendo a informes o resoluciones de autorización, satisfaciendo así el objetivo de ocurrencia. En cambio, si el auditor desea realizar un seguimiento desde la recepción

de esos informes hasta el registro de esas adquisiciones para satisfacer el objetivo de completitud, este proceso se denomina “seguimiento” (o trazabilidad).

Impacto para el auditor: No se debe olvidar que, en algunos casos, los documentos, junto con revelar la información que se busca, deben cumplir ciertas formalidades para su aceptación como evidencia de auditoría. De lo contrario, el auditor deberá valerse de otros medios de verificación independientes que corroboren la información.

Por otro lado, la evidencia documental, ya sea en papel o en soporte electrónico, es más fiable que la obtenida de manera oral, y los documentos originales son más fiables que las fotocopias o los documentos digitalizados sin control de veracidad. Aunque los auditores deben considerar la fiabilidad de la documentación, no están llamados a verificar su autenticidad, ni se espera que sean expertos en autenticación de documentos. En estos casos, se debe recurrir a un especialista forense que cuente con las competencias y recursos técnicos para determinar la autenticidad.

Por último, es posible que los documentos originales no existan, ya sea porque se extraviaron de manera accidental, se destruyeron en forma deliberada o simplemente no están disponibles. En estos casos, una copia sería útil para el auditor, siempre que los datos contenidos en ella puedan contrastarse con otra evidencia (evidencia corroborativa).

- 2. El examen físico:** Es la inspección o recuento por parte del auditor de un activo tangible. Este tipo de evidencia se asocia con mayor frecuencia con el inventario y el efectivo, pero también es aplicable a la verificación de valores, pagarés por cobrar y otros activos fijos tangibles. En la auditoría, existe una distinción entre la inspección de activos, como valores negociables y efectivo, y la inspección de documentos, como cheques cancelados y documentos de venta. Si el objeto que se está examinando, por ejemplo, una factura de venta no tiene valor inherente, la evidencia se denomina documentación.

En general, los estándares mundiales de auditoría se refieren a la inspección de activos físicos y documentos como un tipo de evidencia, pero es útil distinguir entre el examen físico de activos y la inspección de documentos, para ayudar a los auditores a comprender la naturaleza de estos tipos de evidencia.

La inspección es un medio directo para verificar que un activo existe realmente (objetivo de existencia) y se considera uno de los tipos de evidencia de auditoría más fiables. Por lo general, el examen físico es un medio objetivo para determinar tanto la cantidad como la descripción del activo. En algunos casos, también es útil para evaluar el estado o la calidad de un activo. Sin embargo, el examen físico tiene dos claras limitaciones:

- No es suficiente para verificar que los activos existentes son propiedad de la actividad bajo revisión (objetivo de derechos y obligaciones).
- La valoración adecuada no se puede determinar mediante el examen físico (objetivo de precisión y valor realizable).

- 3. La confirmación:** Describe la recepción de una respuesta directa por escrito de un tercero que verifica la exactitud de la información solicitada por el auditor. La respuesta puede ser en papel, electrónica o mediante otro medio, como el acceso directo del auditor a la información en poder del tercero. Un mecanismo es que esa solicitud la haga el propio auditado, quien pide al tercero que responda directamente al auditor. Debido a que las confirmaciones provienen de terceros, son un tipo de evidencia apreciado y utilizado con frecuencia. Sin embargo, las confirmaciones son relativamente costosas de obtener y pueden causar inconvenientes a quienes se les pide proporcionarlas. Por lo tanto, no se utilizan en todos los casos aplicables.

Los auditores deciden si utilizar o no confirmaciones en función de la fiabilidad que requieren, así como de la evidencia alternativa disponible. Por ejemplo, las confirmaciones rara vez se utilizan en la auditoría de adiciones de activos fijos, ya que pueden verificarse adecuadamente mediante la inspección y el examen físico. De manera similar, las confirmaciones no se suelen usar para verificar transacciones individuales entre organizaciones, como transferencias internas, porque el auditor puede utilizar documentos para ese propósito (por ejemplo, una Resolución Exenta). Naturalmente, hay excepciones. Supongamos que el auditor detecta dos compras extraordinarias registradas tres días antes de fin de año. La confirmación de estas transacciones podría ser apropiada.

- 4. Los procedimientos analíticos:** Definidos por las normas de auditoría como aquellas evaluaciones de la información financiera a través del análisis de relaciones plausibles entre datos financieros y no financieros. Un auditor puede comparar, por ejemplo, el porcentaje de variaciones del año en curso con el del año anterior. Los procedimientos analíticos se utilizan ampliamente en la práctica y son necesarios durante las fases de planificación, ejecución y finalización de las auditorías.

Al llevar a cabo procedimientos analíticos en los que la información no auditada del año en curso se compara con la información auditada de años anteriores, se destacan las variaciones. Estos cambios pueden representar tendencias importantes o eventos específicos, los cuales influirán en la planificación de la auditoría. Por ejemplo, un aumento en los porcentajes de compras a lo largo del tiempo puede indicar un despilfarro de recursos o podrían estar correlacionados con los aumentos de programas sociales en los últimos años.

Asimismo, las diferencias significativas e inesperadas entre los datos financieros no auditados y otros datos utilizados en comparaciones se denominan comúnmente “fluctuaciones inusuales”. Estas fluctuaciones ocurren cuando no se esperan diferencias significativas pero existen, o cuando se esperan y no existen. Si la fluctuación es significativa (material), el auditor debería determinar la razón y asegurarse de que la causa es válida y no una irregularidad. Si fuera una irregularidad, se debería “reorientar” el foco hacia procedimientos más detallados que podrían revelar importantes hallazgos.

5. **La indagación:** Es la obtención de información escrita u oral de la actividad bajo revisión en respuesta a las preguntas del auditor. Aunque se obtiene una cantidad considerable de información a través de este procedimiento, por lo general no se puede considerar concluyente porque no proviene de una fuente independiente y puede estar sesgada. Por lo tanto, cuando el auditor obtiene evidencia a través de la indagación, normalmente es necesario obtener evidencia corroborante a través de otros procedimientos. Por ejemplo, si el auditor desea obtener información sobre el método de la actividad bajo revisión para registrar y controlar las operaciones contables, puede comenzar preguntando al auditado sobre cómo funcionan los controles internos, y posteriormente realizar pruebas para verificar si las transacciones se registran (objetivo de integridad) y se autorizan (objetivo de ocurrencia) de la manera indicada.
6. **El recálculo:** Consiste en volver a comprobar una muestra de cálculos realizados por la actividad bajo revisión. Gran parte de los recálculos de los auditores se realiza utilizando hojas de cálculo o software de auditoría especializado.
7. **La reejecución:** Son pruebas independientes realizadas por el auditor de los procedimientos o controles contables de la actividad bajo revisión, que se realizaron originalmente como parte del sistema contable y de control interno de la entidad. Mientras que el recálculo implica volver a comprobar un cálculo, la reejecución implica verificar otros procedimientos. Por ejemplo, revisar el circuito de autorizaciones de compras o gastos extraordinarios. Otro tipo de reejecución consiste en que el auditor verifique las transferencias de información rastreando la información en más de un lugar para asegurar que se registre de manera consistente.
8. **La observación:** Consiste en observar un proceso o procedimiento realizado por otros. Por ejemplo, el auditor puede recorrer las oficinas de la actividad bajo revisión para obtener una impresión general de sus instalaciones u observar si el Centro de Datos está diseñado conforme a los estándares de seguridad de la información.

La observación proporciona evidencia sobre el desempeño de un proceso o procedimiento, pero está limitada al momento en que se lleva a cabo. La observación rara vez es suficiente por sí misma debido al riesgo de que el personal cambie su comportamiento ante la presencia del auditor. Pueden seguir las políticas estatales en ese momento, pero reanudar sus actividades normales una vez que el auditor no esté presente. Por lo tanto, es necesario acompañar las impresiones iniciales con otro tipo de pruebas que las corroboren. La observación es particularmente útil para evaluar la eficacia de los procedimientos de la actividad bajo revisión en el recuento del inventario, así como en muchos otros procedimientos de auditoría.

Cada tipo de evidencia desempeña un papel crucial en respaldar las conclusiones de los auditores y garantizar la exactitud y solidez de sus recomendaciones. Independientemente del tipo, toda evidencia utilizada en auditoría interna debe cumplir con los criterios de

relevancia, fiabilidad y suficiencia para ser considerada válida y confiable. A modo de resumen, se expone la siguiente tabla:

TIPOS DE EVIDENCIAS	DEFINICIÓN	EJEMPLOS
Indagación	Consiste en buscar información de personas conocedoras dentro o fuera de la actividad bajo revisión.	Obtener información escrita u oral de la actividad bajo revisión en respuesta a preguntas específicas durante la auditoría.
Observación	Consiste en observar un proceso o procedimiento realizado por otros.	Observación por parte del auditor del conteo de inventarios realizado por el personal de la actividad bajo revisión, visita a las instalaciones.
Inspección	Consiste en examinar registros, documentos o bienes tangibles.	Revisión de órdenes de venta, facturas de ventas, extractos bancarios, documentos de devolución de clientes, cartas de reclamos de clientes, etc.
Recálculos	Consiste en comprobar la exactitud aritmética de los documentos fuente y registros contables, o en realizar cálculos independientes.	Comprobación de facturas de venta e inventario, adición de diarios y registros subsidiarios, cálculo de gastos de depreciación y gastos prepagados.
Reejecución	Consiste en la ejecución independiente de procedimientos o controles que originalmente se realizaron como parte del control interno de la actividad.	Utilización de CAATs para verificar los controles registrados en la base de datos; validación de la antigüedad de las cuentas por cobrar.
Confirmación	Consiste en la respuesta a una consulta para corroborar información contenida en los registros contables.	Confirmar la existencia de cuentas por cobrar y cuentas por pagar, verificar saldos bancarios con bancos, valor de rescate de instrumentos financieros, etc.
Procedimientos analíticos	Consisten en el análisis de ratios y tendencias significativas, incluida la investigación de fluctuaciones y relaciones inconsistentes con otra información relevante o que se desvían de las cantidades predecibles.	Cálculo de tendencias en las ventas en los últimos años, comparación del índice actual de clientes con el índice de la industria, comparación de presupuestos con resultados reales, etc.

Tabla 1: Resumen tipos de evidencia en Auditoría

Fuente: Elaboración propia

En síntesis:

- La eficacia de los controles internos de la actividad bajo revisión tiene una influencia significativa en la fiabilidad de la mayoría de los tipos de evidencia. Por otro lado, la documentación interna de la entidad con un control interno efectivo es más confiable porque es más probable que los documentos sean precisos. De lo contrario, los procedimientos analíticos no serán una evidencia fiable si los controles que produjeron los datos proporcionan información inexacta.
- Es probable que tanto el examen físico como el recálculo sean altamente confiables si los controles internos son efectivos, pero su uso difiere considerablemente. Esto nos

demuestra que dos tipos completamente diferentes de evidencia pueden ser igualmente confiables.

- La indagación por sí sola no suele ser suficiente para proporcionar pruebas adecuadas que satisfagan cualquier objetivo de auditoría.
- Los dos tipos de evidencia más costosos son el examen físico y la confirmación. El examen físico (inspección de activos tangibles) es costoso porque normalmente requiere la presencia del auditor cuando se está contando un determinado activo. Por ejemplo, el examen físico del inventario puede dar lugar a que varios auditores viajen a lugares geográficos dispersos. Por otro lado, la confirmación es costosa porque el auditor debe seguir procedimientos cuidadosos en la preparación de la confirmación, la transmisión, la recepción y en el seguimiento de las faltas de respuesta y las excepciones.
- La inspección, los procedimientos analíticos, el recálculo y la reejecución son moderadamente costosos. Si la actividad bajo revisión proporciona documentos y archivos electrónicos para el auditor y los organiza para un uso conveniente, la inspección generalmente tiene un costo bastante bajo. Sin embargo, cuando los auditores deben encontrar esos documentos por sí mismos, la inspección puede ser extremadamente costosa. Incluso en circunstancias ideales, la información y los datos de los documentos son a veces complejos y requieren interpretación y análisis. Por lo general, un auditor tarda mucho tiempo en leer y evaluar los contratos de un cliente, los contratos de arrendamiento y las actas de reuniones, si proceden.
- Dado que los procedimientos analíticos son considerablemente menos costosos que las confirmaciones y el examen físico, la mayoría de los auditores prefieren reemplazar estos últimos por procedimientos analíticos cuando es posible. Sin embargo, los procedimientos analíticos requieren que el auditor decida qué procedimientos utilizar, haga los cálculos y evalúe los resultados. Hacerlo a menudo lleva un tiempo considerable. El costo de las pruebas de reejecución depende de la naturaleza del procedimiento que se está probando. Es probable que volver a realizar procedimientos operativos, como la conciliación bancaria de la actividad bajo revisión, lleve un tiempo considerable.
- Los tres tipos de evidencia de menor costo son la observación, las indagaciones de la actividad bajo revisión y el recálculo. Normalmente, la observación se realiza simultáneamente con otros procedimientos de auditoría. Los auditores pueden observar fácilmente si la actividad bajo revisión está siguiendo los procedimientos apropiados en el conteo de un inventario, y al mismo tiempo contar una muestra de este (examen físico). Las indagaciones de la actividad bajo revisión se realizan extensamente en cada auditoría y normalmente tienen un bajo costo, aunque ciertas consultas pueden ser costosas, como lo sería la obtención de declaraciones escritas de la actividad bajo revisión que documentan las discusiones a lo largo de la auditoría. El recálculo, en tanto, suele ser de bajo costo porque implica cálculos simples y rastreo que se pueden hacer a conveniencia del auditor. A menudo, se utiliza un software para realizar muchas de estas pruebas sustantivas.

- En suma, los procedimientos de auditoría son los pasos detallados, generalmente escritos en forma de instrucciones, para la acumulación de evidencia de auditoría. Por lo tanto, deben ser lo suficientemente claros como para permitir que todos los miembros del equipo de auditoría comprendan qué acciones deben llevarse a cabo o qué información se ha recopilado.

Criterios para determinar la idoneidad					
Tipo de evidencia	Independencia de proveedor	Eficacia de los controles internos	Conocimiento directo del auditor	Competencias del proveedor	Objetividad de evidencia
Examen físico	Alto (el auditor lo hace)	Varía	Alto	Normalmente alto (el auditor lo hace)	Alto
Confirmación	Alto	N/A	Bajo	Varía - por lo general alto	Alto
Inspección	Varía - documentos externos son más independientes que los documentos internos.	Varía	Bajo	Varía	Alto
Procedimientos analíticos	Alto/bajo (el auditor lo hace/el cliente responde)	Varía	Bajo	Normalmente alto (el auditor lo hace/ el cliente responde)	Varía: depende de fiabilidad de los datos
Indagación	Bajo (el cliente provee)	N/A	Bajo	Varía	Varía: bajo a alto
Recálculo	Alto (el auditor lo hace)	Varía	Alto	Alto (el auditor lo hace)	Alto
Re-ejecución	Alto (el auditor lo hace)	Varía	Alto	Alto (el auditor lo hace)	Alto
Observación	Alto (el auditor lo hace)	Varía	Alto	Normalmente alto (el auditor lo hace)	Medio

Tabla N°2: Competencia de los tipos de evidencia

Fuente: Alvin A. Arens (†) *et al*, 2017

VI. EL ESTÁNDAR DE LA EVIDENCIA EN LA AUDITORÍA INTERNA

La obtención, análisis y evaluación de la evidencia ha sido tradicionalmente un pilar fundamental en el proceso de auditoría interna. Sin embargo, con la actualización de las Normas Globales de Auditoría Interna (NOGAI), emitidas el 9 de enero de 2024 por el Instituto de Auditores Internos (IIA), el concepto de evidencia se ha expandido para incluir la "información". Esta evolución responde a la necesidad de un enfoque más amplio y flexible en la recopilación de datos, que permita a los auditores abordar de manera efectiva tanto trabajos de aseguramiento, que se enfocan en proporcionar una evaluación independiente, como servicios de asesoramiento, que ofrecen recomendaciones basadas en un análisis más consultivo.

En esta sección exploraremos el concepto de evidencia - o "información"- en el contexto de la auditoría interna, resaltando los cambios clave en las NOGAI, sus implicaciones prácticas y cómo los auditores internos deben adaptarse para cumplir con los nuevos requerimientos.

6.1. El cambio conceptual: de "evidencia" a "información"

El término "información" ha reemplazado en gran medida al de "evidencia" en las Normas Globales de Auditoría Interna. Este cambio refleja una visión más inclusiva y pragmática de los datos que los auditores recopilan y utilizan durante sus trabajos. Mientras que "evidencia" puede entenderse como pruebas concretas y específicas (documentos, registros, informes financieros, etc.), el concepto de "información" abarca tanto estas pruebas tangibles como otras formas de datos cualitativos y cuantitativos.

Por ejemplo, en la norma 14.1 sobre obtención de información para análisis y evaluación, se especifica que los auditores deben obtener la información relevante para evaluar los procesos y controles bajo revisión, lo que incluye no solo la evidencia documental, sino también datos obtenidos mediante entrevistas, observaciones y análisis estadísticos.

Esta ampliación permite a los auditores mayor flexibilidad al evaluar una variedad de situaciones y riesgos, particularmente en entornos complejos o cuando se realizan trabajos consultivos. En estos casos, la información cualitativa puede ser tan valiosa como la cuantitativa, permitiendo emitir juicios más integrales y orientados al valor.

6.2. Importancia de la evidencia en la auditoría interna

La evidencia, ahora denominada "información", sigue siendo crucial para que los auditores internos emitan conclusiones objetivas y fundamentadas. El propósito fundamental de la auditoría interna es proporcionar aseguramiento independiente y objetivo, lo cual solo es posible si las conclusiones están basadas en información confiable y suficiente.

La recopilación de información debe seguir siendo rigurosa y detallada, garantizando que los hallazgos de auditoría sean válidos, relevantes y puedan soportar un análisis crítico. Las Normas Globales de Auditoría Interna insisten en la necesidad de un enfoque sistemático y disciplinado para obtener información, apoyando así la confiabilidad de las auditorías realizadas.

En este contexto, la información recopilada por los auditores debe cumplir con tres criterios fundamentales:

- **Relevancia:** La información debe estar directamente relacionada con los objetivos de la auditoría y ser útil para evaluar los controles y procesos bajo revisión.
- **Fiabilidad:** La información debe ser creíble y verificable, asegurando que proviene de fuentes confiables y que puede ser validada.
- **Suficiencia:** La cantidad de información recopilada debe ser adecuada para sustentar las conclusiones de la auditoría. Es decir, debe haber suficiente información para proporcionar una base sólida para las recomendaciones y decisiones.

Estas características garantizan que la información utilizada sea de alta calidad y útil para los objetivos de la auditoría.

Por ejemplo, en la norma 14.3 sobre evaluación de hallazgos, se señala que los auditores deben evaluar si los hallazgos son significativos y si la información recopilada justifica las conclusiones propuestas. Este enfoque asegura que el auditor pueda proporcionar recomendaciones accionables a la dirección de la actividad bajo revisión con base en un análisis detallado y fundamentado.

6.3. Recolección y análisis de información en la auditoría interna

El proceso de obtención y análisis de información en auditoría sigue una metodología estructurada para garantizar que sea relevante, fiable y suficiente. En el caso de los trabajos de asesoramiento, puede que no sea necesaria la recopilación de evidencias, dependiendo del acuerdo con las partes interesadas relevantes. Las NOGAI exigen que los auditores recopilen la información necesaria para evaluar los riesgos, controles y procesos, utilizando técnicas como la revisión de documentos, entrevistas con personal clave y la observación directa de los procedimientos. A continuación, se destacan algunas de las normas clave relacionadas con este proceso:

- Norma 13.6 sobre programa de trabajo: Establece que los auditores deben preparar un plan detallado para la recolección de información, que incluya las tareas, metodología y herramientas necesarias. El programa de trabajo se basa en la información obtenida durante la planificación de la auditoría, y guía al auditor en la identificación de los elementos clave que deben ser evaluados.
- Norma 14.1 sobre obtención de información para análisis y evaluación: En esta norma se establece que los auditores deben obtener la información necesaria para evaluar los procesos y controles bajo revisión. Este enfoque incluye la recopilación de documentos, entrevistas con el personal relevante y observación directa de los procesos, garantizando una cobertura completa.
- Norma 14.2 sobre análisis y hallazgos potenciales de la auditoría: Una vez recopilada la información, los auditores deben analizarla para identificar hallazgos relevantes y determinar si es necesario realizar recomendaciones para mejorar los controles y la gestión de riesgos.
- Norma 14.4 sobre recomendaciones y planes de acción: Una vez que la información ha sido recopilada y analizada, los auditores deben formular recomendaciones basadas en los hallazgos, apoyando a la organización en la mejora de sus controles y procesos.

6.4. Uso y protección de la información

Además de obtener y evaluar la información, el auditor debe asegurarse de que su uso y manejo se realicen de manera ética y adecuada, como establecen las Normas 5.1 y 5.2, para proteger la confidencialidad y garantizar la integridad del proceso.

- Norma 5.1 sobre uso de la información: Estipula que los auditores internos deben utilizar la información obtenida exclusivamente para los fines del trabajo de auditoría.

Esto significa que toda la información recopilada, sea documental o cualitativa, debe ser empleada únicamente en el contexto de la auditoría para la que fue obtenida, asegurando así que no se use de manera indebida o con fines distintos a los del trabajo.

- **Norma 5.2 sobre protección de la información:** Esta norma subraya la responsabilidad de los auditores de salvaguardar la confidencialidad de la información obtenida durante el proceso de auditoría. La información debe protegerse contra accesos no autorizados o filtraciones, garantizando que los datos sensibles se manejen de acuerdo con los más altos estándares éticos.

Estas normas refuerzan la importancia de manejar la información con integridad, responsabilidad y respetando la confidencialidad, asegurando que el proceso de auditoría mantenga la confianza y transparencia necesarias para ser efectivo.

6.5. Documentación y comunicación de resultados

Una de las responsabilidades críticas del auditor interno es documentar de manera adecuada toda la información recopilada y el análisis realizado. Esto es fundamental no solo para demostrar conformidad con las normas, sino también para garantizar que los resultados puedan ser revisados y utilizados como base para la toma de decisiones estratégicas dentro de la organización.

En la norma 14.6 sobre documentación del trabajo de auditoría, se resalta la importancia de mantener registros claros y completos de todo el trabajo realizado durante una auditoría. Estos registros no solo deben contener la información utilizada para respaldar las conclusiones, sino también cualquier análisis adicional que se haya realizado para evaluar la efectividad de los controles y riesgos.

Además, la Norma 15.1 sobre comunicación final del trabajo establece que los resultados de la auditoría, incluyendo los hallazgos, recomendaciones y planes de acción, deben ser comunicados de manera efectiva a las partes interesadas, asegurando que entiendan claramente las áreas de mejora y los pasos necesarios para mitigar riesgos identificados.

6.6. Consideraciones prácticas para los auditores internos

Para adaptarse a las Normas Globales de Auditoría Interna, los auditores internos deben:

- Ampliar su enfoque: Considerar no solo la "evidencia" documental tradicional, sino también otros tipos de "información", como entrevistas, análisis de datos cualitativos y observaciones, para garantizar una evaluación completa.
- Aplicar escepticismo profesional: Mantener una actitud crítica al evaluar la fiabilidad de la información obtenida, asegurando que sea suficiente y confiable para respaldar las conclusiones.
- Documentar de manera exhaustiva: Asegurarse de que todo el proceso de recolección y análisis de información esté debidamente registrado y documentado adecuadamente.

en los papeles de trabajo, para facilitar la revisión por otros auditores o durante evaluaciones de calidad.

- Respetar la confidencialidad: Utilizar la información únicamente para los fines del trabajo de auditoría y protegerla de accesos no autorizados, en línea con las Normas 5.1 y 5.2.

Como pudimos ver en esta sección, la actualización de las Normas Globales de Auditoría Interna representa un avance importante en la manera en que los auditores internos abordan la recolección y análisis de información. Al ampliar el concepto de "evidencia" a "información", las normas permiten una mayor flexibilidad y adaptabilidad, esencial para realizar auditorías internas efectivas en entornos dinámicos y complejos.

Además, es crucial que la información utilizada en el proceso de auditoría cumpla con los criterios de relevancia, fiabilidad y suficiencia. La relevancia asegura que la información esté directamente relacionada con los objetivos de la auditoría; la fiabilidad garantiza que los datos sean precisos y verificables; y la suficiencia implica que la cantidad de información sea adecuada para respaldar las conclusiones y recomendaciones de manera sólida.

Asimismo, las Normas 5.1 y 5.2 refuerzan la necesidad de que la información recopilada se maneje de manera ética, protegiendo su confidencialidad y asegurando que solo se utilice para los fines establecidos en la auditoría. Esto refuerza la confianza en los resultados de la auditoría interna y asegura la transparencia y responsabilidad en el proceso.

Para los auditores internos, la combinación de estos enfoques refuerza la importancia de obtener y evaluar información confiable para respaldar conclusiones objetivas y ofrecer valor a la organización, cumpliendo con los más altos estándares éticos y profesionales.

VII. EL VALOR PROBATORIO DE LA EVIDENCIA DE AUDITORIA EN UN JUICIO

Recientemente, hemos analizado cómo el término "información" ha sustituido de manera significativa al de "evidencia" en el ámbito de aplicación de las Normas Globales de Auditoría Interna. Sin embargo, en el contexto legal Meneses Pacheco⁷ hace la distinción entre ambos términos, destacando que la "información" abarca de manera general los hechos importantes que influyen en decisiones clave dentro de un proceso judicial, una definición que bien podemos extrapolar al contexto organizacional. Por su parte, la "evidencia" se considera una "palabra relacional" que se utiliza específicamente en el "contexto de la argumentación", ya sea en un juicio o, para un auditor, en la justificación de hallazgos. De este modo, la "información" puede tener un "rol potencial" como "evidencia", es decir, como fuente de información relevante para afirmar o refutar una proposición de hecho, ya sea en un proceso judicial o en un informe de auditoría, en nuestro caso.

⁷ MENESES PACHECO, CLAUDIO, 2008. "fuentes de prueba y medios de prueba en el proceso civil", Revista Ius et Praxis, Vol. 14(2), <https://dx.doi.org/10.4067/S0718-00122008000200003>.

7.1. Concepto y objeto de la prueba

Como acertadamente lo señala la profesora Carmen Vázquez⁸, el término “prueba” es de por sí ambiguo. Ella lo explica de manera sencilla y clara, considerando que el público objetivo no está familiarizado con estas cuestiones legales. Hace una distinción entre los elementos de juicio, la práctica y el resultado probatorios.

Atendiendo al objeto que regulan las normas jurídicas, la prueba se puede clasificar en tres categorías:

- (i) Reglas sobre los medios de prueba
- (ii) Reglas sobre la práctica de las pruebas admitidas
- (iii) Reglas sobre el resultado de las pruebas admitidas y practicadas

En tal sentido, el Derecho establece que las pruebas deben cumplir con ciertos requisitos fundamentales:

- a) Que la admisión de todos los medios de prueba sea relevante para demostrar la veracidad de las afirmaciones sobre los hechos. Esta proposición es similar a lo que se espera de un auditor al recabar la evidencia de auditoría.
- b) Que la práctica de los elementos de prueba se admita, pues no tendría sentido que se admitan si luego no se valoran. Este hecho distingue claramente entre la evidencia de auditoría y la prueba legal.
- c) Que los elementos admitidos y practicados sean evaluados de forma racional por un juez designado ad hoc.

Algunos autores señalan⁹ que la prueba es cualquier elemento que permite evidenciar, dar fe o certificar una situación, es decir, todo aquello que es apto para rememorar un hecho no presente. Ahora bien, en el ámbito judicial, también se denomina prueba al medio a través del cual el litigante presenta al juez la verdad del hecho afirmado; por ejemplo, documentos, dictámenes periciales, declaraciones de testigos o confesiones. Igualmente, se denomina prueba a la actividad o procedimiento desarrollado al ofrecer o producir un medio probatorio.

En el plano de la prueba legal, judicial o procesal -dicho en un sentido amplio y sin entrar en un análisis más técnico, propias del mundo jurídico- identificamos tres elementos que configuran la prueba propiamente dicha: el objeto de prueba, el órgano de prueba y los medios de prueba.

- (i) El objeto de prueba sería la cosa, el hecho, la circunstancia o el acontecimiento cuyo conocimiento es necesario y se debe acreditar en un proceso legal determinado. Si se

⁸ VÁSQUEZ, CARMEN, 2015, “De la prueba científica a la prueba pericial”, Marcial Pons, Ediciones Jurídicas y Sociales, España.

⁹ ARROYO, JENNIFER, 2014, “Similitudes y Diferencias entre la Evidencia de Auditoría y la Prueba en el Procedimiento Judicial o Administrativo”, Revista Nacional de administración, Vol. 5 (2).

tratase de un hecho delictivo, serían las circunstancias que lo motivan, sus autores, la extensión del perjuicio causado, entre otros, los que precisamente se deben probar. En palabras simples, el objeto de prueba responde a la pregunta: ¿qué debe probarse?

- (ii) El órgano de prueba se refiere a toda persona física encargada de suministrar el conocimiento de los hechos, tales como los testigos presenciales y los peritos, por ejemplo, aquellos vinculados con la labor de auditoría que han elaborado algún informe, o bien, han de pronunciarse sobre un tema en controversia en vía jurisdiccional, administrativa, penal y/o civil. Estas personas también podrían ser llamadas a rendir testimonio y declarar sobre los hallazgos y conclusiones de su informe de auditoría o pericial, según corresponda. De manera sencilla, el órgano de prueba responde a la pregunta: ¿Quién debe probar ese objeto de prueba?
- (iii) Los medios de prueba hacen referencia al aporte de conocimiento al proceso judicial sobre un objeto de prueba, pudiendo ser el testimonio o el informe presentado por el perito-auditor. Estos medios de prueba pueden tomar la forma de declaración en juicio, opiniones técnicas, dictámenes u otros informes de auditoría elaborados como producto del trabajo del auditor, que contribuyen al proceso legal como medios probatorios. Sin embargo, será el juez quien valorará y apreciará el trabajo desempeñado por ese auditor, y determinará cuándo y cómo se incorporarán al proceso, sea como testimonio simple (al inicio), testimonio experto (al final), documental o pericial (al inicio o al final, según corresponda).

La Ley, mediante disposiciones del Código de Procedimiento Civil y de Procedimiento Penal, reconocen una serie de medios probatorios, como elementos comunes, siendo posible encontrar:

- La prueba documental o instrumental.
- La prueba de testigos.
- La prueba confesional de parte (solo en sede civil; en sede penal es la “declaración del imputado”).
- La prueba biológica (ADN y corporal, solo en sede penal).
- La prueba pericial (informe de peritos oficial o de parte).
- Las presunciones judiciales (prueba indiciaria).
- La inspección personal del tribunal.
- Otros medios probatorios tecnológicos (solo en sede penal: películas cinematográficas, fotografías, fonografías, videgrabaciones, versiones taquigráficas, etc.).

De los medios de prueba comentados, haremos referencia a aquellos que pueden afectar al rol del auditor interno. Estos son los siguientes:

A. El auditor interno como testigo experto

La figura del testigo-perito proviene de los sistemas jurídicos de países de habla inglesa, donde se combinan los elementos de la prueba testimonial y la prueba pericial (el informe de peritos). Para poder comprender esta instancia, es necesario precisar las diferencias de ambos roles:

- El testigo se refiere a hechos que ha conocido por medio de sus sentidos, sobre lo que ha visto, escuchado, percibido, y da su versión de los mismos.
- El perito es un técnico que, mediante un informe pericial, ofrece su apreciación y valoración sobre los hechos, basándose en criterios técnicos, cuya opinión técnica ilustra al juez en temas ajenos al derecho.

En suma, el testigo-perito es un testigo porque ha de tener una relación directa, histórica y extraprocesal con los hechos. La relación del perito con los hechos, a diferencia de lo que sucede con el testigo, deriva de un encargo de la parte o del tribunal en relación con el proceso que quiere iniciarse o que ya está en curso. El testigo-perito, al igual que el testigo ordinario, no es sustituible, pues es la persona que ha percibido el hecho. Además, en el caso del testigo-perito, puede valorarlo desde un punto de vista científico, técnico, artístico o práctico porque posee conocimientos de esta naturaleza. En consecuencia, no puede admitirse la declaración en el juicio, en calidad de testigo-perito, de un experto que no tiene relación previa con los hechos, pues no se trata de “personas que tengan noticia de hechos controvertidos relativos a lo que sea objeto del juicio” ((DPEJ)).

De ahí que, si la peritación practicada se lleva directamente a un juicio, mediante el interrogatorio al experto sin la previa aportación del informe escrito, se puede privar a la parte contraria de esa garantía que supone el conocimiento anticipado del informe. Es decir, se atentaría contra el principio de contradicción y, de paso, se estaría ante la inobservancia de las garantías procesales.

Por su parte, el Código de Procedimiento Penal, en su párrafo 6 del Libro Tercero, sobre juicio oral, establece que:

“El Ministerio público y los demás intervinientes podrán presentar informes elaborados por peritos de su confianza y solicitar que estos sean citados a declarar en el juicio oral, acompañando los comprobantes que acrediten la idoneidad profesional.

Procederá el informe de peritos en los casos determinados por la ley y siempre que para apreciar algún hecho o circunstancia relevante para la causa fueren sean necesarios o convenientes conocimientos especiales de una ciencia, arte u oficio.

Los informes deberán emitirse con imparcialidad, ateniéndose a los principios de la ciencia o reglas del arte u oficio que profesare el perito.”

En cuanto a la admisibilidad del informe de peritos, el artículo 316 del Código de Procedimiento Penal, prescribe que:

“El juez de garantía admitirá los informes y citará a los peritos cuando, además de los requisitos generales para la admisibilidad de las solicitudes de prueba, considere que los peritos y sus informes otorgan suficientes garantías de seriedad y profesionalismo.”

Asimismo, los peritos no podrán inhabilitarse. Sin embargo, durante la audiencia del juicio oral, podrán dirigírseles preguntas orientadas a determinar su imparcialidad e idoneidad, así como el rigor técnico o científico de sus conclusiones.

En el campo de auditoría interna el rol de testigos-perito, puede desempeñarse por el auditor interno al elaborar un informe de auditoría, donde se les consulte sobre el proceso de auditoría, la determinación del campo de estudio, la fuente de la información, las pruebas sustantivas realizadas, y otros hechos que no siempre están plasmados en el informe final. También podrían ser consultados sobre aspectos técnicos como las normas de auditoría aplicadas o los procedimientos contables asociados, estén o no incluidos en el informe.

B. El consultor técnico

Según el diccionario panhispánico del español jurídico (DPEJ), un consultor técnico es un experto en una ciencia, arte o técnica que, a instancia de parte, puede intervenir en el proceso penal para presenciar las operaciones periciales, formular observaciones sobre las mismas y hacer conclusiones sobre la prueba pericial en las audiencias. Sin embargo, esta figura no es propiamente un medio de prueba, pero resulta relevante incluirla en este análisis, pues puede ser otro rol que podría desempeñar un auditor en un proceso judicial o administrativo.

En definitiva, el consultor técnico es un especialista en un área técnica que asesora a las partes, ya sea al abogado acusador o al abogado defensor, con el fin de que este pueda plantear preguntas, objeciones y alegatos a un perito o testigo perito en aspectos técnicos de la declaración.

Otra cuestión de gran importancia es establecer adecuadamente aquellos hechos que sí requieren prueba¹⁰, esto es, deben probarse aquellos hechos de manifiesta controversia y que no han sido aceptados por las partes. Estos deben referirse a hechos sustanciales, pertinentes y controvertidos. Esta es una materia que predomina en los procesos contenciosos administrativos y judiciales de índole civil. Se entiende por estos:

- **Hecho sustancial:** Es aquel que forma parte esencial del conflicto, de tal manera que sin su prueba no se puede adoptar resolución alguna.
- **Hecho pertinente:** Es aquel que, sin ser parte esencial del conflicto, se vincula a él y es necesario para la resolución del órgano jurisdiccional.
- **Hecho controvertido:** Es aquel que genera discrepancia en cuanto a su existencia o la forma en que ocurrió.

¹⁰ JIMÉNEZ BARAHONA, MAGDALENA *et al*, 2004, “Aspectos Generales de la Prueba y los Medios de Prueba”, Material Docente, Escuela de Derecho, Universidad de Chile, U Cursos.

En ámbito penal, no es una cuestión discrecional del juez ni de las partes si un delito es “sustancial o controvertido”, ya que la ley establece qué constituye un delito, definido como “toda acción u omisión voluntaria penada por la ley” (artículo 1 del Código Penal). Por tanto, el juez verificará si se cumplen los presupuestos legales para establecer la responsabilidad del autor.

7.2. Valoración de la evidencia: La regla de la sana crítica

Sin pretender excedernos a los propósitos de este documento técnico, conviene comprender aspectos elementales sobre uno de los mecanismos que poseen los sentenciadores al momento de valorar la prueba, particularmente la prueba pericial. En efecto, el trabajo de un auditor podría referirse a la aportación de informes técnicos en alguna instancia judicial que permitan al juzgador apreciar determinados hechos, que requieren la opinión experta de un especialista. El mecanismo recurrente por la judicatura para evaluar este tipo de hechos es mediante los informes técnicos de peritos y cuyo instrumento de valoración es llevado a cabo mediante la aplicación de la Regla de la “Sana Crítica”.

La experiencia litigiosa en Chile ha adoptado durante décadas, con cierta afinidad, esta regla valorativa. Un ejemplo de ello se observa en el artículo 297 del Código Procesal Penal, artículo 14 de la Ley 18.287, que establece los procedimientos ante los juzgados de Policía Local; artículos 455, 456 y 459 letra d) del Código del Trabajo; el artículo 32 de la Ley 19.968 que crea los Tribunales de Familia, así como otras tantas leyes al respecto.

Con todo, en lo que respecta a la prueba pericial, la regla de la sana crítica ha sido por excelencia el principio rector del juzgador al momento de someter el informe de peritos a las reglas de valoración. Nuevamente, esto desprendido de los mismos cuerpos legales que aluden a esa regla procesal¹¹.

Ahora bien, debemos comprender qué es la regla de sana crítica. Una acepción señala:

“La sana crítica es aquella que nos conduce al descubrimiento de la verdad por los medios que aconseja la recta razón y el criterio racional puesto en juicio. Es analizar sinceramente y sin malicia las opiniones expuestas acerca de cualquier asunto. Las reglas que la constituyen no están expuestas en la ley. Se trata de un proceso intelectual interno y subjetivo, o sea, es materia de apreciación y, por lo mismo, de hecho, que corresponde exclusivamente a los jueces del fondo” ¹².

¹¹ NINO-MORIS, CHRISTIAN, 2023, “La Concepción del Fraude en la Profesión del Auditor y Algunas Implicancias Jurídicas en el Derecho Penal Económico, y Su Impacto en la Evacuación del Informe Pericial Contable”, tesina como requisito para optar al grado de Magíster en Derecho Penal Económico y de la Empresa, UNIVERSIDAD SAN SEBASTIÁN (obra inédita no publicable).

¹² Citado por LARROUCAU TORRES, JORGE, 2012, en EXCMA. CORTE SUPREMA, uno de abril de 1974, REVISTA DE DERECHO Y JURISPRUDENCIA, Tomo 68 (1971), Sección 1ª, p.76, citado en Rioseco (1995) t.II N°694 p. 378.), https://derechopedia.cl/Sana_cr%C3%ADtica [Último acceso: Junio 2024].

La Academia Judicial de Chile ha confirmado lo anterior¹³, al señalar que el sistema de sana crítica puede tenerse como aquel que permite la valoración de la prueba en conciencia, pero de una forma racional y que es la vertiente procesal del énfasis de la utilización de la racionalidad para valorar la prueba. Esto es, se trata de conseguir una valoración probatoria objetiva, lógica e intersubjetivamente controlable.

Existe profusa jurisprudencia judicial al respecto en esta materia, donde nuestra Excelentísima Corte Suprema se ha pronunciado en los siguientes términos:

“Doctrina y jurisprudencia están contestes en que la apreciación de la prueba en conciencia significa autorizar a los tribunales para hacer de esta una apreciación racional, con recta intención y conforme a la sana crítica, sin estar obligados a someterse a las normas legales establecidas para valorarla. [...] Ahora bien, la evaluación de la prueba en conciencia no libera al tribunal de respetar las demás reglas sustantivas en materia probatoria, tales como, cuáles son los medios de prueba, su admisibilidad y la carga o distribución [de ésta], lo que conduce a sostener que conculcados los cánones que gobiernan dichos tópicos puede ser objeto de control por la vía extraordinaria de la casación”¹⁴.

En el mismo orden de ideas, ese mismo máximo tribunal ha señalado:

“...la apreciación de la prueba en este tipo de materias, según lo dispone la ley, debe efectuarse conforme al sistema de la sana crítica, el que, a su vez, se traduce en un proceso mental que realiza el juez, que consiste en un examen de los elementos probatorios del juicio, el cual debe conducir lógicamente a la conclusión que se encuentra vertida en la decisión que adopte, de manera tal que pueda justificarse ante los destinatarios de la misma, tarea que, como reiteradamente se ha sostenido, es ajena a las facultades de este tribunal de casación, y solo será abordable en aquellos casos en que el juzgador, al realizar la labor de valoración de prueba, quebrante los principios que conforman el sistema de la sana crítica, esto es, los de la lógica, máximas de la experiencia o los conocimientos científicamente afianzados”¹⁵.

7.3. El rol del auditor en un juicio

¿Por qué es importante para el auditor conocer cómo el juzgador -ya sea administrativo o judicial- valora sus informes técnicos en el eventual transcurso de un proceso contencioso? La respuesta radica en que las normas globales de auditoría interna exigen al auditor aplicar juicio profesional en el ejercicio de su labor. Dicho juicio se refiere a la capacidad del auditor para tomar decisiones informadas y objetivas, fundamentadas en su experiencia, conocimientos y competencias adquiridas. Esta habilidad resulta esencial

¹³ ACADEMIA JUDICIAL DE CHILE, 2022, “Valoración Probatoria: Exigencias Legales, Jurisprudenciales y Doctrinales”, Juan S. Vera Sánchez.

¹⁴ Sentencia de la EXCMA. CORTE SUPREMA, 06 de septiembre de 2016, Causa ROL 9086-2015, considerando Séptimo.

¹⁵ Sentencia de la EXCMA. CORTE SUPREMA, 04 de agosto de 2014, Causa ROL 15256-2014, considerando Quinto.

para enfrentar situaciones complejas, seleccionar los enfoques más adecuados y llegar a conclusiones razonables, especialmente en el análisis de riesgos y controles.

Aunque la definición literal de "juicio profesional" no aparece explícitamente en el glosario de las Normas, su práctica permea toda la estructura normativa. Esto subraya la importancia de un análisis crítico y fundamentado para garantizar el éxito de la auditoría interna. El concepto está íntimamente ligado a la Norma 4.2 sobre cuidado profesional debido, la cual obliga a los auditores internos a actuar con diligencia y escepticismo profesional, asegurando así la calidad y la imparcialidad de su trabajo. Además, este enfoque es clave no solo para evitar sesgos, sino también para preservar la objetividad durante las evaluaciones.

En el contexto de las Normas Internacionales de Auditoría el juicio profesional se define como "La aplicación de la formación práctica, el conocimiento y la experiencia relevantes, en el contexto de las normas de auditoría, contabilidad y ética, para la toma de decisiones informadas acerca del curso de acción adecuado en función de las circunstancias del trabajo de auditoría" (NIA Sección AU 200.13).

No obstante, lo anterior no siempre coincidirá con los elementos que la regla de la sana crítica exige al juzgador. En suma, el juzgador valorará un informe técnico a través de los tres principios centrales que conforman la regla de la sana crítica, esto es:

1. Los principios de la lógica,
2. Las máximas de la experiencia, y/o
3. Los conocimientos científicamente afianzados.

Estos elementos exigen al juez, al momento de revisar la prueba, la observancia de cuestiones específicas que no admitan contradicción. Por tanto, si un informe técnico es evacuado por el auditor y ofrecido como medio de prueba, deberá, previamente, requerirse la opinión del área jurídica respectiva, de manera que la constatación de los hechos a informar no sobrepase las competencias del auditor¹⁶.

Esto incluye evitar la incorporación de pruebas con vulneración de garantías fundamentales de las personas, así como pruebas obtenidas mediante actos ilícitos o derivadas de actos legales cuya fuente adolezca de vicios de ilicitud. En cualquier caso, si los informes técnicos son considerados como pruebas ilícitas, la calificación corresponderá al juez competente. En suma, los auditores deben realizar sus investigaciones/indagaciones -que derivan en la evacuación de informes técnicos- valiéndose de medios idóneos y respetando los derechos fundamentales de las personas.

Habiendo analizado criterios, la pregunta que subyace es: ¿bajo qué circunstancias podría llegar un informe técnico de un Auditor a manos del juzgador? Para responder esta interrogante destacaremos dos escenarios hipotéticos de acción:

¹⁶ Véase como argumentos de referencia en cuanto a rol del auditor, Ordinario 3274: 2017 <https://www.dt.gob.cl/legislacion/1624/w3-article-112439.html> [Último acceso: Junio 2024].

1. Procedimiento administrativo y sancionatorio administrativo

En relación con el debido proceso y, tratándose del derecho administrativo, el legislador ha consagrado el derecho a producir la prueba en los términos de la Ley 19.880 sobre Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado.

Este cuerpo normativo regula expresamente un único medio probatorio: los informes, encargados a otros servicios u organismos, los cuales son facultativos –por regla general– y no vinculantes para la administración, constituyendo una regla epistémica, porque otorgan información que permite alcanzar la verdad sobre los hechos¹⁷..

A su vez, los hechos que el administrado plantea como hechos relevantes, mediante alegaciones o presentaciones, no pueden ser rechazados en forma categórica por la administración sin que exista una adecuada fundamentación, por cuanto para una correcta apreciación de la realidad sobre la cual la administración debe ejercer la potestad es preciso analizar conforme a las reglas de la sana crítica la pertinencia y sustancia de estos.

Al respecto, la Contraloría General de la República ha señalado que por muy amplia que sea la discrecionalidad otorgada a un órgano de la administración, ella deberá siempre ejercerla de un modo racional y razonado, lo cual se concreta en materia de prueba en la obligación de emitir una resolución fundada en los casos que la prueba sea calificada como improcedente o innecesaria¹⁸

Por otro lado, el artículo 15 de la Resolución N°510 de 2013, que aprueba el reglamento de sumarios instruidos por la Contraloría General de la República, prescribe que, para la mejor dilucidación de los hechos investigados, con motivo de un sumario administrativo llevado a cabo por la Contraloría General de la República se podrán solicitar informes periciales¹⁹. En tanto, el DFL 29 de 2004, de Hacienda, que fija texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre estatuto administrativo, en cuanto a los procesos sumariales administrativos efectuados por los distintas reparticiones públicas²⁰, la Ley no establece medios de prueba en específico, limitándose el artículo 138, inciso

¹⁷ DROGHETTI FUENTES, PIA ALEJANDRA & PÉREZ JIMÉNEZ, MARIA JOSÉ, 2017, “La Actividad Probatoria en el Derecho Administrativo Sancionador a la luz de la Ley de Bases de los Procedimientos Administrativos”, FACULTAD DE DERECHO, DEPARTAMENTO DE DERECHO PÚBLICO, UNIVERSIDAD DE CHILE (Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales).

¹⁸ AGUIRREZABAL, MAITE & FLORES, JUAN C., 2021, “La prueba como Elemento Esencial del Debido Procedimiento Administrativo”, REVISTA DE DERECHO ADMINISTRATIVO ECONÓMICO, REDAE, N° 33, Facultad de Derecho, Pontificia Universidad Católica de Chile.

¹⁹ Artículo 15: “En la etapa indagatoria, el fiscal instructor podrá solicitar la ratificación de las denuncias que se hubieren formulado y tomará declaraciones a los presuntos implicados, a los afectados y a los testigos, cuantas veces sea necesario, para la mejor dilucidación de los hechos investigados. Asimismo, podrá solicitar informes periciales, realizar inspecciones personales y careos, adjuntar documentos y, en general, practicar todas las diligencias necesarias tendientes a establecer los hechos y la participación de los funcionarios eventualmente comprometidos.”

²⁰ Artículo 1: “Las relaciones entre el Estado y el personal de los Ministerios, Intendencias, Gobernaciones y de los servicios públicos centralizados y descentralizados creados para el cumplimiento de la función administrativa, se regularán por las normas del presente Estatuto Administrativo, con las excepciones que establece el inciso segundo del artículo 21 de la ley N°18.575.”

segundo del Estatuto Administrativo a indicar que si el inculpado solicitare rendir prueba, el fiscal señalará el plazo para tal efecto, el que no podrá exceder en total de veinte días. No obstante, la Ley no hace ninguna referencia a los medios de prueba en específico, se entiende que es posible presentar cualquier medio probatorio siempre que estos sean de carácter lícito.

2. Proceso acusatorio penal

El artículo 84 del citado Estatuto Administrativo señala que los funcionarios públicos, incluidos los auditores internos del sector público, pueden intervenir ante tribunales de justicia como parte, testigo o perito, respecto de hechos de los que hubieren tomado conocimiento en el ejercicio de sus funciones, o bien declarar en juicio en que tenga interés el Estado o sus organismos, previa comunicación y autorización de su superior jerárquico.

Lo anterior, se correlaciona de manera directa con lo establecido en el artículo 321 del Código Procesal Penal (CPP), que prescribe que el Ministerio Público (la Fiscalía), podrá presentar como peritos a los miembros de organismos técnicos que le presten auxilio en su función investigadora, ya sea que pertenezcan a la policía, al propio Ministerio Público o a otros organismos estatales especializados en tales funciones.

Asimismo, el artículo 319 del Código de Procedimiento Penal, establece que la declaración de los peritos en la audiencia del juicio oral (como testigo experto) consistirá en una breve exposición del contenido y las conclusiones de su informe, para el posterior examen y contra examen de los litigantes. Siguiendo, en su rol de testigo experto, si se ausentará o negare a comparecer, será merito suficiente para la aplicación de sanciones corporales (arresto por hasta veinticuatro horas o una reclusión menor en su grado medio a máximo) y pecuniarias (pago de las costas y/o de una multa de hasta 15 unidades tributarias mensuales).

7.4. Los indicios y la prueba indiciaria en la función del auditor

Otro aspecto para tener en cuenta en el ejercicio de la función del auditor es respecto a los indicios y la prueba indiciaria. Comprender esto ayuda a la red de auditores a ejercer un mejor escepticismo profesional y, por ende, una mejor conducción de su juicio profesional en la obtención de evidencia, que en definitiva redundará en la preparación de sus informes.

El diccionario de la RAE define el término “indicio” como aquel “fenómeno que permite conocer o inferir la existencia de otro no percibido”. En tanto, el diccionario panhispánico del español jurídico (DPEJ) lo define como aquella “circunstancia que apunta a la existencia de un hecho probablemente delictivo («indicios racionales de criminalidad») y justifica la incoación de la investigación, su continuación o la exigencia de prestación de fianza para asegurar responsabilidades pecuniarias, circunstancia que, en conjunción con otras, permite deducir razonadamente que se ha producido un determinado hecho e incluso tenerlo por probado”.

Ahora bien, desde el punto de vista criminalístico, como la investigación forense, el uso de la palabra “indicio” se considera inapropiado, ya que equivale en realidad al termino en español “evidencia”. De ahí que es común que en los medios de comunicación televisivos se muestren los hallazgos de las policías con un banner que dice “EVIDENCIA”. Es decir, este tipo de indicios solo nos permite establecer la relación entre las personas y objetos del sitio del suceso, pero no nos indica si la persona es culpable o no del hecho criminal.

Álvarez Saavedra²¹ nos explica muy bien la naturaleza de los indicios criminales. Éste nos señala que el indicio es aquella circunstancia de la que se induce otra y que nos lleva, en último caso, a obtener la prueba. El indicio se asocia a la acción o señal que da a conocer sobre algo que está oculto o todo hecho conocido que demuestra la existencia de otro desconocido.

Siguiendo con este autor, el indicio es el medio por el cual se llega a cosas ciertas utilizando el razonamiento inductivo, deductivo y analógico, mientras que la prueba demuestra una evidencia. Pero diríamos que debe tener el “ungimiento” del juzgador, porque no es cualquier evidencia. En criminalística se le conoce también como evidencia física, evidencia material. De ahí que se asocien los indicios a todo objeto, instrumento, huella, marca, rastro, señal o vestigio que se usa o se produce en la comisión de un hecho delictivo, y cuyo estudio da las bases científicas para encaminar una investigación criminal.

En tanto, “prueba indiciaria”, siguiendo lo señalado por el diccionario panhispánico del español jurídico (DPEJ): “Medio probatorio consistente en la apreciación de la realidad de los hechos por la convicción que resulta de determinados indicios. Para que los indicios puedan ser utilizables como prueba, han de estar plenamente probados, no pueden tratarse de meras sospechas, y debe explicitarse el razonamiento en virtud del cual, partiendo de los indicios probados, se ha llegado a la conclusión de que el sujeto realizó la conducta infractora. «Cuando de blanqueo de capitales procedentes de delito contra la salud pública se trata, una consolidada jurisprudencia ha consagrado un triple pilar indiciario para sustentar su existencia. Sin perjuicio de que pudieran concurrir adicionales que ratifiquen la convicción, la prueba indiciaria será:

- a) El incremento inusual del patrimonio o el manejo de cantidades de dinero que, por su elevada cantidad, dinámica de las transmisiones y tratarse de efectivo, pongan de manifiesto operaciones extrañas a las prácticas comerciales ordinarias.
- b) La inexistencia de negocios lícitos que justifiquen el incremento patrimonial o las transmisiones dinerarias.
- c) La constatación de algún vínculo o conexión con actividades de tráfico de estupefacientes o con personas o grupos relacionados con las mismas [u otro delito base]»”.

²¹ ÁLVAREZ SAAVEDRA, FÉLIX, 2008, “Diccionario de Criminalística: Los secretos de las Investigaciones de la Policía Científica”, Editorial Planeta S.A., España.

Pues bien, dicho lo anterior, ¿qué indicios son comunes a los cuales debe prestar atención el auditor? A modo de ejemplos, se tienen los siguientes:

A. Señales cualitativas²²

Se trata de señales relacionadas con aspectos como las características de las personas o la organización; por ejemplo, un cambio en los hábitos de un funcionario que se puede percibir cuando comienzan a incurrir en gastos muy lujosos.

- Sanciones legales en el pasado.
- Malos hábitos financieros (muchas deudas o un estilo de vida muy lujoso).
- Bajos estándares éticos.
- Directivos o funcionarios que no toman sus vacaciones.
- Alta rotación de directivos, funcionarios o consultores.
- Conflictos en el consejo ad hoc (según la repartición pública).
- Deficiencias en el gobierno corporativo.
- Falta de consejeros independientes.
- Falta de regulaciones de prevención del fraude (por ejemplo, un código de ética).
- Ausencia de un canal para los denunciantes.
- Auditores inadecuados para trabajos de alta complejidad.
- Conflictos con los auditores.
- Operaciones inusuales o complejas que son difíciles de entender.
- Dificultades para cumplir con cláusulas resolutorias de contratos.
- Exigencias poco razonables planteadas al auditor, como restricciones de tiempo poco realistas para la finalización de la auditoría o la emisión del informe de auditoría.
- Actitud prepotente de la actividad bajo revisión en su trato con el auditor, especialmente cuando ello conlleva intentos de influir en el alcance del trabajo o en la selección o continuidad del personal asignado al trabajo de auditoría o consultado durante el trabajo.
- Incentivos agresivos por resultados de cumplimiento a corto plazo.
- Sistemas ineficaces de contabilidad e información, incluidas situaciones que implican deficiencias significativas en el control interno.

B. Señales cuantitativas

Las cuentas proporcionan señales de alerta fuera de lo común para la comprensión de un “hombre prudente”, entre otras:

- Falta de conciliación completa y oportuna de los activos de la actividad bajo revisión.
- Partidas de conciliación significativas no explicadas.
- Ausencia de documentación sobre las transacciones oportuna y adecuada.
- Transacciones que no se han registrado íntegra u oportunamente, o que se han registrado incorrectamente en lo referente a la cantidad o importe, periodo contable, clasificación o política de la entidad.

²² Adaptados de: PARRONDO, LUZ & AMAT, ORIOL (Editors), 2024, “Comprehensive red flag model for accounting fraud detection using qualitative and quantitative variables”, Research Handbook on Financial Accounting, Edward Elgar Publishing, y de NIA Sección AU 240.

- Saldos o transacciones sin justificación documental o autorización.
- Ajustes de última hora que afectan significativamente a los resultados.
- Evidencia de acceso de los empleados a sistemas y registros incongruentes con el acceso que necesitan para desempeñar sus tareas autorizadas.
- Documentos que parecen haber sido alterados.
- Disponibilidad únicamente de fotocopias y documentos transmitidos electrónicamente en los casos en que cabe esperar que existan documentos originales.
- Discrepancias inusuales entre los registros de la entidad y las respuestas de confirmación.
- Desaparición de inventarios o de activos físicos de magnitud significativa.
- Evidencia electrónica no disponible o pérdida de ella, cuando ello resulte incongruente con las prácticas o políticas de conservación de registros de la entidad.

VIII. ASPECTOS FUNDAMENTALES DE LA EVIDENCIA DIGITAL

En el presente capítulo se abarcarán varios tópicos específicos referidos a la evidencia digital y que ayudarán a la comprensión de su importancia en el ejercicio de las funciones del auditor, así como a advertir cuándo sería pertinente la asistencia de un informático forense; todo ello con el objeto de preservar la integridad de los datos que puedan emanar de los distintos dispositivos electrónicos.

8.1. Definición de evidencia digital

Como primera cuestión, se debe comprender qué se entiende por “evidencia digital” o “evidencia electrónica”. Existen numerosas publicaciones que abordan distintas dimensiones, dependiendo del énfasis del estudio.

En este sentido, se dice que la información almacenada electrónicamente es “digital” porque ha sido convertida en dígitos, específicamente unidades binarias representadas por unos y ceros, que se almacenan y recuperan a través de un conjunto de instrucciones denominado software o código.

Por su parte, la norma chilena NCh-ISO 27037:2015, que adopta el estándar internacional ISO/IEC 27037:2012, proporciona directrices para la identificación, recolección, adquisición y preservación de evidencia digital. Según esta norma, la evidencia digital se define como información o datos almacenados o transmitidos en formato digital que pueden ser usados en una investigación o procedimiento legal.

Ahora, un consenso mundial sobre la materia, surgido en la Conference of International Investigators (CII, 2021), señala que la “evidencia digital” se define como la información y datos de valor potencial para una investigación que se almacenan o transmiten en forma digital. La evidencia digital se diferencia de la evidencia tradicional por algunas de las siguientes razones:

- a) A menudo es muy compleja, está dispersa en diferentes ubicaciones físicas o virtuales y requiere experiencia y herramientas para recopilarla.

- b) Puede modificarse fácilmente de forma accidental o intencionada, posiblemente sin dejar ningún rastro.
- c) Puede copiarse y distribuirse fácilmente, lo que presenta desafíos para preservar la confidencialidad.
- d) Puede ser de naturaleza temporal. Los registros de red, el historial de navegación en Internet, las publicaciones en redes sociales, los mensajes instantáneos, los datos almacenados en caché y los datos eliminados pueden perderse si no se conservan de manera oportuna.

La evidencia digital es tan valiosa como la evidencia física tradicional. A veces, es incluso más valiosa, ya que puede ser más directamente incriminatoria o más fácilmente disponible que la evidencia física. La evidencia digital se puede encontrar en todos los medios digitales, incluidos discos duros, teléfonos móviles/inteligentes, CD-ROMs, tablets, tarjetas de cámaras digitales, dispositivos GPS y otros.

Al igual que otros tipos de pruebas, la evidencia digital enfrenta dos cuestiones²³²⁴ de particular importancia que deben considerarse antes de que pueda admitirse en un tribunal (al menos en lo que respecta a buenas prácticas, ya que en Chile se opera de manera más flexible en estas materias).

La primera es que, dado que la evidencia digital, al considerarse “evidencia”, debe obtenerse legalmente con una orden judicial adecuada. Sin embargo, esto crea un gran dilema al manejar dispositivos digitales, ya que a menudo se requiere una “investigación digital”, que no es tan robusta desde el punto de vista forense como para formar una hipótesis sobre el caso y la participación del sospechoso. En efecto, una cosa es el dispositivo y otra lo que está contenido en él. Por ejemplo, se ha dado el caso en que la policía registra un teléfono —sin protección de contraseña— sin la correspondiente orden judicial, lo que lleva a preguntarse si el teléfono y su contenido pueden llegar a ser una prueba legal al acceder de manera ilegal. Para qué decir si es un auditor quien lo hace en una etapa prejudicial; esto significaría destruir la evidencia.

La segunda cuestión es que la evidencia digital debe obedecer al cumplimiento de reglas de admisibilidad, al igual que la evidencia física, cuando se utiliza en un tribunal de justicia (véase acápite 8.2.). En general, la evidencia digital se refiere principalmente a dos aspectos: integridad y autenticidad. La literatura especializada ya se refiere ampliamente a estos atributos.

Por consiguiente, la evidencia digital satisface la “integridad” si no se modifica durante los procesos de adquisición y análisis. La capacidad de confirmar la integridad de la evidencia se denomina “autenticidad”. En particular, la autenticidad también puede referirse a la

²³ KÄVRESTAD, JOAKIM, 2020, “Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications”, Second Edition, Springer Nature Switzerland.

²⁴ Inciso uno, artículo 2, Ley 21.459:2022: “Acceso ilícito. El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales”.

exactitud de la información y la confiabilidad de la fuente. Por otro lado, para establecer la autenticidad de la evidencia, es importante documentar la cadena de custodia desde el sitio del suceso (CSI, Crime Scene Investigation) hasta el tribunal (una suerte de trazabilidad) mediante los análisis. Esto es particularmente crucial y desafiante para la evidencia digital, ya que también es única porque tiene necesidades de integridad mucho mayores y más específicas en comparación con la evidencia tradicional. En efecto, es mucho más difícil destruir o manipular un documento de papel que modificar los metadatos en un archivo crítico.

Sin embargo, dado que la evidencia digital puede modificarse en la práctica, los abogados han argumentado que es inherentemente menos confiable que otras formas de evidencia. Por lo tanto, debe exigirse una “cadena de custodia” para preservar la integridad de la evidencia digital a medida que pasa por las etapas de investigación y su posterior exhibición en los tribunales de justicia.

8.2. Aspectos legales esenciales sobre la evidencia digital²⁵

Haciendo un breve estado del arte, encontramos las siguientes disposiciones en asuntos de “procedimientos digitales” en materia jurídico-contenciosa. Por ejemplo, en el Procedimiento Civil, CPC (donde supletoriamente aplican para los procedimientos administrativos), el artículo 348 bis de ese cuerpo legal establece una audiencia de percepción documental cuando las partes ofrezcan documentos electrónicos, sin perjuicio de las normas sobre la prueba complementaria de autenticidad.

En tanto, respecto a los aspectos procesales en el ámbito penal, los artículos 187, 217 y 333 del Código del ramo se refieren a los documentos (“los instrumentos”) como medios de prueba para acreditar la comisión de un ilícito y todo aquello “electrónico” que sea apto para producir fe.

Los cuerpos legales antes señalados -procesal civil y penal- comparten algo en común: no se hacen cargo de las exigencias mínimas que deben satisfacer las partes al momento de ofrecer la prueba electrónica ante el juzgado o tribunal respectivo. La ley solo se hace cargo del “qué”, pero no del “cómo” ofrecer esos documentos electrónicos ni cómo deben prepararse. Tampoco el legislador hace referencia a reglamentos en cuanto a las directrices que deben seguirse para el proceso de preparación de la prueba documental electrónica. Estos reglamentos deberían ya existir, al menos para los formatos básicos de documentos electrónicos.

A modo de ilustración, algunos de los déficits que se han constatado en la preparación, gestión y ofrecimiento de la evidencia electrónica se relacionan con cuestiones que el auditor debe advertir y perfeccionar en su comprensión:

- La realización de imágenes forenses de dispositivos de almacenamiento digital no es lo mismo que hacer una copia doméstica de datos. Aquí se recomienda que se respeten

²⁵ NINO-MORIS, CHRISTIAN, 2020, “Tribunales de justicia y evidencia digital: una oportunidad que se vislumbra por Covid-19”, <https://www.elmercurio.com/legal/movil/detalle.aspx?Id=908836&Path=/0D/DE/>

las directrices contenidas en la NCh-ISO 27037:2015 sobre la identificación, recopilación, adquisición y preservación de evidencia digital (véase más adelante).

- El manejo adecuado de la “cadena de custodia” es esencial para ciertas piezas de prueba electrónica es de cuidado²⁶.

El uso excesivo de las planillas electrónicas como medio de prueba directa, que en cierta jurisprudencia judicial internacional se han desestimado como medios idóneos de prueba debido a que no existe certeza de que los datos producidos en dichas planillas hayan seguido un protocolo de integridad informática (por ejemplo, que los datos no sean manipulables). Específicamente, esto último está referido a establecer la verdadera autoría de las planillas electrónicas (archivos no repudiados), por cuanto estas toman por defecto, por ejemplo, como autor el nombre consignado en el equipo computacional (sistema operativo o proceso de instalación del software) y no necesariamente ese nombre guarda relación con el autor de los registros electrónicos (datos) consignados en esas planillas. En esa misma línea de razonamiento, por regla general las planillas electrónicas no contienen un registro fidedigno (llámese “archivos logs”) sobre las personas que intervinieron en su manipulación. No obstante, se ha detectado casos en que los tribunales han validado su admisibilidad en razón que la parte afectada no ha procedido a impugnarlas en función de lo establecido por el artículo 348 bis del CPC.

El problema es mayor cuando los archivos han sido descargados desde un software licenciado hacia un formato de planillas electrónicas, donde el usuario o administrador de ese sistema no es la misma persona que manipula o procesa las planillas. En nuestro país, estas planillas se ofrecen como documentos en soporte papel o viceversa: se imprimen en papel, pero la fuente de los datos proviene de dichas planillas, lo que constituye una forma de “burlar” la norma.

- El uso masivo de documentos en formato PDF (Portable Document Format) en los procesos judiciales y en la Administración Pública presenta varios desafíos, tales como: la descripción de la resolución (ppp o dpi), la orientación de las páginas (90° y 180° casos típicos), la compresión de los datos contenidos y la naturaleza de los documentos capturados en formato PDF (origen o fuente de captura).

A continuación, se abordan dos problemas frecuentes relacionados con los documentos en formato PDF:

- a) Tipología de los documentos: La producción de un PDF no se limita a ver y abrir un archivo almacenado en ese formato, sino de conocer cómo fue su proceso de producción. En este sentido, es importante distinguir entre un documento “escaneado en PDF” y un documento en “True PDF”.

²⁶ Un ejemplo de ello se aprecia en Causa ROL C-2069-2020, 4º Juzgado Civil de Santiago, donde el tribunal dispuso: “comparezca el perito [contable], a objeto de obtener copia del dispositivo electrónico custodiado bajo el N°XXX-2022. Se hace presente al perito que, para tal objeto, debe apersonarse al tribunal con un pendrive en blanco, en el que se le entregará copia del contenido custodiado.”

El primero se refiere a aquellos que, al convertirse a un formato PDF, el contenido se "congela" como una imagen que es capturada como en una cámara fotográfica, sin que exista una capa de texto –leíble– subyacente. En otras palabras, la imagen capturada no se puede editar en forma de texto en una primera instancia.

El segundo se refiere a aquellos documentos que se crean directamente desde cualquier software de escritorio o, simplemente, mediante la función "imprimir" dentro de una aplicación del software (impresora virtual). Este documento sí puede leerse de mejor manera porque, desde su origen, viene editable, sin que sea necesario aplicar un proceso de reconocimiento de textos. Ello redundará en una notable calidad visual, de impresión y captura de datos. Por tanto, la cuestión no queda supeditada a una distinción semántica, ya que una adecuada identificación de estos documentos incide en la forma de procesar la información y la obtención de datos útiles al proceso. Por lo tanto, las mayores probabilidades de éxito en la captura de los datos están dadas para aquellos documentos del tipo "True PDF".

- b) Calidad del escaneo de documentos: Durante el proceso de captura de datos surgen inconvenientes prácticos en la producción de documentos escaneados, debido a que no cumplen con las especificaciones mínimas de DPI (puntos por pulgada), lo que afecta la calidad de los documentos digitalizados antes de ser presentados al tribunal (u otra instancia contenciosa). Por ejemplo, se han procesado documentos a 96 DPI, lo que dificulta la lectura óptica de caracteres y reduce la precisión en la recuperación de datos. La "regla" indica que cuanto mayor es la resolución de escaneo, mejor es la calidad del procesamiento; por ello, las buenas prácticas sugieren que un documento escaneado, convertido a PDF, tenga entre 200 y 300 DPI, según las distintas fuentes generadoras de la información (formatos). Sin embargo, a menudo se descuidan estos estándares de calidad por limitaciones en la capacidad del dispositivo digital o por las exigencias de los proveedores de Firma Electrónica Avanzada.

8.3. Modelos de análisis de informática forense

En cuanto a los modelos de análisis de la evidencia digital, se pueden distinguir los siguientes procedimientos forenses, que la literatura técnica cita tanto en publicaciones de revistas indexadas como en manuales sobre la materia:

El primer modelo pertenece a Kruse & Heiser, llamado “Las Tres A”: *Adquisición, Autenticación y Análisis de la evidencia*²⁷:

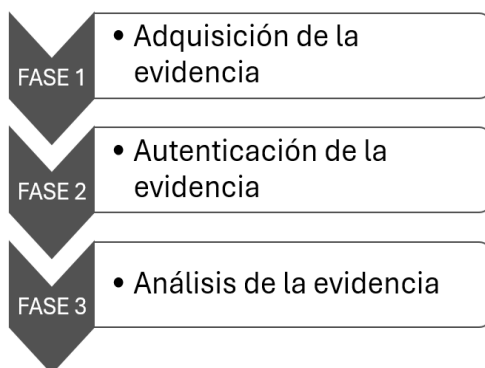


Figura 2: Modelo de Kruse y Heiser
Fuente: KRUSE, WARREN G. & HEISER, JAY G. (2002)

El segundo modelo está atribuido a Universidad de Yale, desarrollado por Eoghan Casey en 1997 (mejorado en el año 2011²⁸), quien por aquel entonces era el supervisor de seguridad de los sistemas de TI de dicha universidad. Es muy similar a un proceso y procedimientos estándar de respuesta a incidentes y consta de siete etapas: preparación, levantamiento (CSI), documentación (cadena de custodia), preservación, examen y análisis, reconstrucción, e Informe de resultados:

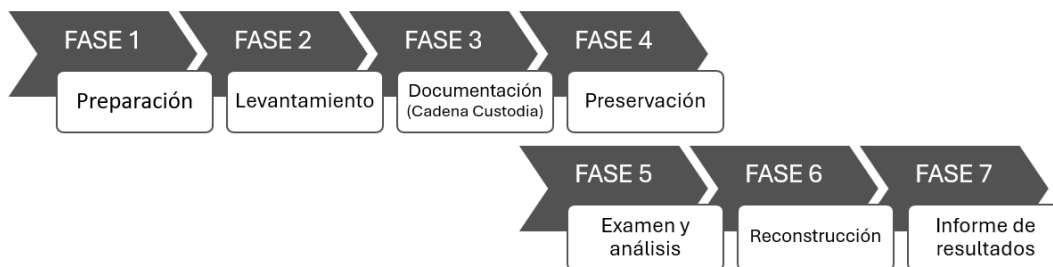


Figura 3: Modelo de Casey
Fuente: CASEY, E.(2011)

²⁷ KRUSE, WARREN G. & HEISER, JAY G., 2002, “Computer forensics: incident response essentials”, Addison-Wesley, Estados Unidos.

²⁸ CASEY, EOGHAN, 2011, “Digital evidence and computer crime: Forensic science, computers and the internet”, 3rd Edition, Academic Press, Estados Unidos.

El tercer modelo corresponde a Rodney McKemmish (1999) de la Policía de Australia (AFP). Este modelo comprende cuatro fases a lo largo de la investigación: Identificación, Preservación, Análisis y Presentación de la evidencia digital:



Figura 4: Modelo de McKemmish
Fuente: MCKEMMISH, R. (1999)

De los modelos antes mencionados, podemos ver claramente algunos datos interesantes:

- Hay algunas similitudes entre ellos a pesar de que son de diferentes autores y partes del mundo.
- Cada modelo tiene énfasis en alguna etapa específica.
- Aunque existen algunas similitudes y diferencias, el objetivo principal es extraer la evidencia digital que se pueda introducir en un proceso judicial; esta debe ser admisible, respetar los derechos de los intervinientes y ser obtenida de manera lícita.

Como se mencionó anteriormente, en Chile existe la NCh-ISO 27.037:2015 sobre “directrices para la identificación, recopilación, adquisición y preservación de evidencia digital”. Tal como lo estipula la norma, esta entrega orientación para los siguientes dispositivos y/o funciones que son usadas en diversas circunstancias:

- Medios de almacenamiento digital usados en computadores estándar, tales como: discos duros, disquetes, discos ópticos y magneto-ópticos, dispositivos de almacenamiento de datos con funciones similares.
- Teléfonos móviles, asistentes digitales personales (PDAs), dispositivos electrónicos personales (PEDs), tarjetas de memoria.
- Sistemas de navegación móvil, cámaras de video y digitales (incluyendo circuito cerrado de televisión)
- Computadores estándar con conexiones de red.
- Redes basadas en TCP/IP y otros protocolos digitales.
- Dispositivos con funciones similares a las nombradas anteriormente.

Por último, en el apéndice de este documento técnico se establecen los “Principios generales para la evidencia digital”, reconocidos por la Conference of International Investigators, 2021, que integran entidades tales como:²⁹The International Monetary Fund, The Organization of American States, The Inter-American Development Bank, The World Trade Organization y The United Nations; de los cuales Chile es adherente a las recomendaciones que estas IGOs (organizaciones intergubernamentales) efectúan a sus países partícipes.

²⁹ <https://www.ciinvestigators.org/participating-organisations/>.

8.4. Análisis de informática forense más recurrentes

Ahora es el turno de identificar los análisis de informática forense más recurrentes en la práctica³⁰:

a) Análisis forense de memoria RAM

Este término se refiere a la aplicación de técnicas forenses en cualquier memoria volátil, que incluye RAM, cachés (de todos los niveles) y registros. El análisis forense de la memoria debe realizarse durante el análisis en vivo, ya que el contenido de la memoria volátil se pierde permanentemente cuando se apaga el sistema.

b) Análisis forense del sistema operativo (OS)

El análisis de archivos logs (“huella digital”) es una parte importante del análisis forense de un sistema operativo, ya que los formatos de los archivos de registro difieren enormemente entre ellos. El equivalente de Linux al registro de Windows no funciona de igual manera. Para realizar análisis forenses de sistemas operativos, el investigador debe tener un conocimiento profundo y exhaustivo de estos, así como la capacidad de comprender el significado de los registros generados.

c) Análisis forense multimedia

Este análisis forense se refiere a la aplicación de técnicas informáticas forenses en archivos que contienen más datos audiovisuales que texto, tales como grabaciones de sonido, archivos de música, videos e imágenes. Hay muchos casos posibles en los que los archivos multimedia serían útiles como prueba: los archivos de música pirateados, las grabaciones de sonido y video de delitos, y las imágenes pornográficas ilegales son buenos ejemplos de ello.

d) Análisis forense de correspondencia electrónica

Como se mencionó respecto de los dispositivos móviles, se puede encontrar mucha información incluso en los correos electrónicos más comunes. Las personas malintencionadas pueden recopilar direcciones de correo electrónico (tanto del remitente como del destinatario) y comenzar a enviar spam a estas cuentas con la esperanza de realizar phishing o propagar malware. Las direcciones IP pueden ser obtenidas como parte de una misión de reconocimiento, lo que ayuda al atacante a visualizar cómo está construida la red. Los encabezados de los correos contienen una gran cantidad de información útil para un hacker, incluso antes de considerar el contenido del correo, cuya filtración podría tener consecuencias en el mundo real, como ya ha ocurrido en el ámbito local.

³⁰ LIN, XIAODONG, 2018, “Introductory Computer Forensics: A Hands-on Practical Approach”, Springer Nature Switzerland.

Sin embargo, los correos electrónicos son igualmente útiles para los investigadores forenses, ya que pueden ser analizados para descubrir detalles sobre el remitente y sus motivaciones, e incluso presentados como prueba judicial en un tribunal.

Un ejemplo de esto es realizar un análisis heurístico del encabezado (esencialmente los metadatos del correo) para asegurarse de que se ajusta al formato especificado por el proveedor de servicios de correo utilizado para enviarlo: si un correo afirma haber sido enviado por un servicio específico, pero el conjunto de campos y/o el orden de su encabezado es diferente o contiene información inesperada (como un número entero donde debería haber un nombre), esto indica que el correo ha sido falsificado.

e) Análisis forense financiero

Las actividades delictivas financieras (como una categoría de los delitos económicos) están aumentando a tasas insospechadas. En efecto, a medida que los medios digitales se utilizan para almacenar grandes cantidades de información financiera en sistemas múltiples y complejos, las tendencias en las actividades fraudulentas mutan. Ya no se trata de simples falsificaciones en los libros de contabilidad y sus comprobantes, sino que se ha avanzado a nuevos fraudes, como la modificación de archivos financieros y la eliminación o alteración de datos importantes. Para enfrentar estos desafíos, las técnicas de auditoría forense están en constante evolución. Por ello, las técnicas de data mining se han utilizado ampliamente para la detección de fraudes.

Por otra parte, según cómo un dispositivo digital haya estado involucrado en una investigación forense, se puede establecer su intervención en la comisión de un delito:

- El dispositivo se utiliza directamente como una herramienta para realizar actividades delictivas, como un micrófono oculto que se emplea para escuchar una conversación privada.
- El dispositivo es víctima de un delito, como cuando a un usuario le roban la identidad en línea o es afectado por un keylogger que roba contraseñas.
- El dispositivo es periférico al delito y, sin quererlo, reúne evidencia útil para la investigación. Un ejemplo sería cuando un turista toma una foto en el momento en que ocurre un delito y, como resultado, el sospechoso aparece en la imagen.

8.5. La evidencia digital en auditoría interna

En la era digital, los auditores internos enfrentan nuevos desafíos al gestionar la evidencia digital, un recurso crucial para respaldar sus hallazgos y conclusiones. Con la creciente dependencia de los sistemas de información, la recolección, análisis y preservación de datos digitales se ha vuelto esencial para asegurar la transparencia, la integridad y la disponibilidad de la información auditada.

Las directrices técnicas contenidas en las Guías de Auditoría para Seguridad de la Información y Ciberseguridad (GASIC)³¹ desarrolladas por el CAIGG y las Guías de Auditoría de Tecnología Global (GTAG)³² emitidas por el IIA, no abordan explícitamente el tema de la evidencia digital. Sin embargo, varias de estas guías tratan aspectos relacionados con la gestión y auditoría de tecnologías de la información que pueden implicar el manejo de evidencia digital.

Sin embargo, ambas guías permiten a los auditores internos tener un enfoque integral que aprovecha tanto la especialización del contexto público como las prácticas globales en auditoría de TI, facilitando una cobertura más completa y efectiva en la gestión de riesgos de ciberseguridad y la evidencia digital. Adaptar estos lineamientos a la práctica diaria no solo mejora la efectividad de las auditorías, sino que también refuerza la integridad y la protección de la información digital en las organizaciones.

Como se mencionó anteriormente la evidencia digital se refiere a información almacenada electrónicamente que puede ser utilizada para sustentar hallazgos, conclusiones y recomendaciones en una auditoría interna. Esta evidencia resulta particularmente útil en el análisis de incidentes de ciberseguridad, el seguimiento de transacciones y la identificación de patrones inusuales que puedan indicar riesgos o amenazas. La capacidad de los auditores internos para manejar la evidencia digital con precisión y rigor es fundamental para asegurar la calidad de la auditoría y, en última instancia, la credibilidad de los hallazgos.

En este contexto, las GASIC abordan distintos aspectos de la seguridad de la información y la ciberseguridad, proporcionando una base sólida para la recolección y preservación de evidencia digital. Estas guías no solo alertan sobre la importancia de la evidencia digital, sino que también enfatizan la necesidad de una metodología rigurosa para asegurar que esta sea confiable y esté protegida de manipulaciones. En incidentes de seguridad, el rol de la evidencia digital es crucial para documentar y comprender lo sucedido. La GASIC sobre gestión de incidentes de seguridad subraya la importancia de procedimientos claros para identificar y conservar la evidencia, así como la necesidad de que los auditores reciban capacitación en técnicas de preservación que aseguren que la evidencia permanezca intacta y confiable.

La gestión de riesgos de seguridad es otro pilar en la recolección de evidencia digital. Las GASIC guían a los auditores en la identificación de riesgos que puedan comprometer la

³¹ <https://www.auditoriainternadegobierno.gob.cl/gasic-guias-de-auditoria-para-seguridad-informacion-y-ciberseguridad/>

³² <https://www.theiia.org/en/standards/2024-standards/global-guidance/>

integridad y disponibilidad de la evidencia. Es esencial evaluar el ambiente de control y asegurarse de que existan salvaguardas que prevengan la alteración o eliminación accidental de la información clave para sus conclusiones. Los controles de acceso también son vitales para proteger la evidencia digital, ya que limitan el acceso a esta información, permitiendo solo a personal autorizado manipular la información relevante.

Por otro lado, las GTAG ofrecen lineamientos más específicos sobre cómo auditar tecnologías y procesos de análisis de datos, herramientas fundamentales en el manejo y examen de evidencia digital. El uso de tecnologías de análisis permite a los auditores no solo recolectar evidencia, sino también explorar patrones de datos, detectar anomalías y realizar auditorías más precisas. Una recomendación central de las GTAG es el empleo de herramientas de análisis que aseguren la integridad de la evidencia digital, permitiendo que cualquier hallazgo basado en estos análisis sea trazable y verificable.

Asimismo, las GTAG subrayan la importancia de que los auditores comprendan los fundamentos técnicos de los sistemas de información que gestionan la evidencia digital. Esta comprensión facilita la identificación de puntos críticos donde la evidencia podría ser vulnerable, permitiendo que los auditores implementen medidas preventivas efectivas. En cuanto a la gestión de identidades y accesos, las GTAG enfatizan la necesidad de contar con controles sólidos para garantizar que la evidencia digital solo esté disponible para aquellos que la necesitan en el contexto de la auditoría.

Por su parte, tanto la GTAG sobre "Auditoría de Operaciones de Ciberseguridad: Prevención y Detección" del IIA describen cómo las actividades de monitoreo de seguridad cibernética incluyen el seguimiento de registros de eventos de sistemas y análisis forense de tráfico de red para identificar posibles incidentes de seguridad. Estas prácticas generan rastros de evidencia digital, como registros de conexiones no autorizadas, elevaciones o cambios de permisos de usuario en el sistema, que son esenciales para detectar y analizar incidentes cibernéticos.

8.6. Buenas prácticas para el manejo de evidencia digital en auditoría interna

El manejo de evidencia digital exige una combinación de conocimientos técnicos y buenas prácticas. Desde la perspectiva de las GASIC y GTAG, se destacan varios aspectos:

- **Documentación y cadena de custodia:** Una cadena de custodia bien documentada es fundamental para cualquier auditoría. Cada movimiento y acceso a la evidencia digital debe ser registrado, lo cual no solo garantiza la trazabilidad de la información, sino que también previene manipulaciones y asegura que la evidencia se mantenga en su estado original.
- **Uso de herramientas especializadas:** Las herramientas de forense digital juegan un rol crucial al preservar la integridad de los datos. Estas herramientas permiten a los auditores capturar y analizar evidencia digital sin comprometer su autenticidad, asegurando que sea admisible tanto en auditorías internas como en investigaciones formales.

- **Capacitación constante:** En un entorno digital en constante evolución, los auditores deben mantenerse actualizados en técnicas de análisis de datos y ciberseguridad. La capacitación continua es vital para que los auditores comprendan y apliquen correctamente los principios y técnicas de preservación de evidencia digital.

8.7. *Algunas consideraciones prácticas en manejo de la evidencia digital*

Existen algunos problemas comunes en la recolección de evidencia digital que pueden afectar la integridad y la confiabilidad de esta. Algunos de estos problemas más comunes incluyen³³:

- Contaminación de la evidencia: La evidencia digital puede contaminarse si no se siguen procedimientos adecuados para recolectarla. Por ejemplo, el uso inadecuado de herramientas de recolección o el acceso no autorizado a la evidencia pueden alterar los datos originales.
- Falta de la cadena de custodia: La cadena de custodia es esencial para garantizar la confiabilidad de la evidencia digital. Sin un registro detallado de cómo se ha manejado la evidencia, es difícil determinar si ha sido alterada o modificada.
- Problemas de almacenamiento: La evidencia digital debe almacenarse de manera segura y protegida contra el acceso no autorizado. Sin embargo, a menudo se producen problemas de almacenamiento, como el daño físico de los dispositivos de almacenamiento o la pérdida de datos debido a un problema técnico.
- Dificultad para autenticar la evidencia: Autenticar la evidencia digital puede ser difícil debido a la complejidad de los metadatos y otros aspectos técnicos de la evidencia. Sin una correcta autenticación, es difícil garantizar que la evidencia no se ha alterado ni modificado.
- Problemas de presentación: Presentar la evidencia digital de manera clara y convincente puede ser difícil debido a la complejidad de los datos y la falta de comprensión técnica del personal judicial.
- Falta de entrenamiento adecuado: La falta de entendimiento de la tecnología y los dispositivos utilizados para almacenar, recolectar y transmitir la evidencia digital puede llevar a la pérdida de información importante y, por ende, a la pérdida de pruebas en un proceso judicial, lo que puede determinar ganar o perder un juicio.

En resumen, la recolección de evidencia digital es un proceso complejo y delicado que requiere una gran precisión y atención al detalle. Muy especialmente, debe llevarse a cabo por profesionales idóneos.

³³ DAMIAN MANFREDI, MARIANO, 2023, "Introducción a la evidencia digital", MINISTERIO PÚBLICO Fiscal de la Ciudad Autónoma de Buenos Aires - MPF CABA.

Luego de exponer los aspectos esenciales en la comprensión y tratamiento de la evidencia digital, se presentan algunas recomendaciones³⁴ a considerar por los auditores internos:

- Las evidencias originales nunca deben utilizarse para desarrollar procedimientos de análisis.
- Hay que considerar que la evaluación de la evidencia podría descubrir indicios relativos a actividades delictivas (Por ejemplo, delitos funcionarios), por lo que ello podría configurar la obligación de denuncia, según lo establece el artículo 175 y siguientes del CPP.
- Si se encuentra evidencia que no ha sido autorizada para registro por parte de la autoridad respectiva, póngase en contacto con los asesores legales para obtener ayuda si es necesario. En estos casos, nunca actúe por iniciativa propia.
- Una vez dispuesta la evidencia digital, debería llevarse a cabo un proceso de protección contra escritura, a fin de preservar y proteger la evidencia original; todo con la debida asistencia experta.
- No cambie nunca el estado actual (encendido/apagado) del dispositivo.
- En ningún momento deje el dispositivo abandonado o sin asegurarlo adecuadamente.
- No copie nada hacia o desde el dispositivo. Una vez que se tengan los dispositivos cuestionados, un especialista forense acreditado creará una imagen forense verificada de cada elemento de evidencia, siempre que sea posible. Una imagen forense no es lo mismo que una copia doméstica de datos.
- No acceda a nada que contenga el dispositivo, tales como imágenes, aplicaciones o archivos, sin antes utilizar una herramienta de bloqueo contra escritura.
- En el caso de los teléfonos móviles, si no están cargados, no deben cargarse. Si el teléfono está encendido, apáguelo para evitar la eliminación o sobreescritura de datos debido a su inicio automático.
- No se deben conectar medios de almacenamiento externos al dispositivo. Asegúrese de que la computadora no esté apagada; si es necesario, déjela en modo hibernación.
- No confíe en aquellos profesionales que no tengan formación en informática forense ni competencias en el manejo de evidencia digital. La unidad de auditoría interna respectiva debería contratar los servicios de especialistas forenses. El proceso de conservación y análisis de datos requiere el conocimiento de un profesional de

³⁴ Tomado de un número de fuentes: FORENSIC EXAMINATION OF DIGITAL EVIDENCE: A GUIDE FOR LAW ENFORCEMENT, 2004, US Department of Justice, Office of Justice Programs, National Institute of Justice; Counter Fraud Authority; Forensicsguru.com.

investigación forense que abarque desde la recuperación de la información borrada hasta la prestación de la respectiva declaración en juicio (si se llega a esa instancia).

- Nunca reasigne el dispositivo cuestionado. Los departamentos de TI suelen reasignar los dispositivos a otros usuarios por diversas razones. Si bien esto puede parecer inofensivo, puede tener consecuencias catastróficas, como borrar evidencia crítica almacenada en esos dispositivos. El uso de profesionales forenses permite llevar a cabo imágenes de manera rápida y segura de los datos, lo que permite posteriormente reasignar el dispositivo.

Siempre tener en cuenta:

- Tome una fotografía de todas las evidencias que forman parte del levantamiento de estas (CSI).
- El tiempo es esencial cuando se trata de la evidencia digital. Recorra al área legal tan pronto como tenga conocimiento de la situación.
- Cuando sea posible, solicite las contraseñas, datos de inicio de sesión y códigos PIN de teléfonos móviles.
- No comente con nadie ningún asunto relacionado con una investigación forense que no necesite saberlo. Es posible que esas personas estén involucradas o tengan algún tipo de conexión con los autores o sospechosos.

8.8. Competencias de los auditores gubernamentales para la obtención de evidencia electrónica de auditoría

Un estudio llevado a cabo en su oportunidad por académicos de la Universidad de Santiago³⁵ detectó algunas problemáticas asociadas al respecto, las cuales podrían estar presentes, en la actualidad, ya sea en mayor o menor medida, y afectar el desempeño de los auditores internos del sector público:

- Los datos recolectados a través de esta investigación demostraron que los auditores internos del sector gubernamental, objeto del estudio, en términos generales, no poseían el conocimiento ni las competencias necesarias para obtener evidencia electrónica de auditoría.
- Los hallazgos evidenciaron que la población de estudio carecía tanto del “saber qué” como del “saber cómo” en relación con el manejo de los nueve elementos de la evidencia tradicional y electrónica (por ejemplo: origen, alteración, aprobación, completitud, lectura, formato, almacenamiento o archivo, disponibilidad, accesibilidad y firma), así como de los seis criterios de confiabilidad y calidad presentes en la evidencia electrónica (autenticación, autorización, integridad, no repudio, confidencialidad y accesibilidad).

³⁵ Caldana, D., Correa, R., & Ponce, H. (2007). Competencias de los auditores gubernamentales para la obtención de evidencia electrónica de auditoría. *Contaduría y Administración*, 223, 9-31. Universidad Nacional Autónoma de México.

- Menos del 10 % de la población contaba con las competencias procedimentales requeridas, es decir, poseían las competencias mínimas para obtener evidencia electrónica de auditoría confiable y de calidad.
- El restante 90 % manifestó confusiones o ausencia de estas competencias. La falta de competencias específicas para obtener evidencia electrónica confiable podría incrementar los niveles de riesgo de auditoría, al aumentar los riesgos inherentes, de control y de detección, especialmente este último, debido a la dificultad de obtener rastros o pistas de auditoría en las transacciones electrónicas.

A partir de lo expuesto, los autores, en función de las particularidades que distinguen a la evidencia electrónica de aquella en papel, desarrollaron un modelo de competencias conceptuales y procedimentales requeridas por los auditores para asegurar la obtención de evidencia de auditoría confiable y de calidad.

Descriptores	Competencias conceptuales	Competencias procedimentales	Competencias actitudinales
Familiaridad en el trabajo con documentos electrónicos.	Conocimiento y uso de los tipos de documentos tributarios electrónicos y de la organización.	—	• Debido cuidado profesional. • Objetividad. • Actitud crítica. • Capacidad de análisis. • Capacidad de abstracción. • Perseverancia. • Escepticismo, no creer sólo lo que parece a primera vista en pantalla. • Disposición y actitud a aprender cosas nuevas, en especial tecnologías de información. • Flexibilidad de pensamiento. • Actitud favorable hacia la actualización permanente.
Dificultad en el trabajo con documentos electrónicos.	Grado de conocimiento de dificultades en el trabajo con documento electrónico.	—	
Identificar medios de soporte de documentos electrónicos.	Conocimiento de los medios de soporte de un documento electrónico.	—	
Identificar tipos de formatos de documentos electrónicos.	Conocimientos sobre formatos de documentos electrónicos: texto, presentación, video, imágenes, entre otros.	—	
Determinar origen del documento electrónico recibido.	Conocimientos de los elementos que distinguen la evidencia electrónica de auditoría (Autenticación, Autorización, Integridad, No-Repudio, Confidencialidad, Accesibilidad).	Examinar, verificar y determinar el origen, emisor o creador del documento electrónico.	
Determinar integridad del documento electrónico.		Evaluar y determinar la completitud, alteración o modificación en el contenido del documento electrónico.	
Relacionar aprobación documento electrónico con funcionario que cuenta con facultades.		Examinar y verificar la identificación del funcionario que aprueba actos en el documento electrónico recibido.	

Descriptor	Competencias conceptuales	Competencias procedimentales	Competencias actitudinales
Asegurar visualización fiel del contenido de documento electrónico.		Examinar y determinar si la representación en el computador corresponde fiel e íntegramente al contenido del documento electrónico.	
Obtener accesibilidad adecuada y segura al contenido del documento electrónico.		Acceso seguro a los repositorios formales y posteriormente, al contenido del documento electrónico.	
Reconocer Firma Electrónica Simple en documento electrónico.		Examinar y distinguir si un documento electrónico cuenta con Firma Electrónica Simple formal y válida.	

Tabla 3: Competencias requeridas para obtener evidencia electrónica de auditoría
Fuente: CALDANA, D., CORREA, R., & PONCE, H. (2007)

IX. EJEMPLOS DE CASOS PRÁCTICOS FOCALIZADOS

9.1. Diferencia entre evidencia y prueba

Para delinear la distinción entre "evidencia" y "prueba legal", se presentarán dos situaciones reales, que ilustran cómo la aplicación de estos conceptos puede variar según la etapa procesal y el contexto específico.

a) Caso Práctico N° 1

El siguiente caso corresponde a un proceso judicial relacionado con una investigación de alta connotación pública, donde surgieron denuncias sobre la posible pérdida de correos electrónicos relevantes pertenecientes a un ejecutivo, los cuales habían sido incautados por la Fiscalía. Por lo que el juez ordenó a una unidad especializada verificar la integridad de la evidencia y emitir un informe. Aunque inicialmente hubo dudas sobre la manipulación de la información, la Fiscalía aclaró que la evidencia no se había perdido, sino que permanecía íntegra en un servidor incautado, pues el acceso se gestionaba mediante copias forenses disponibles para revisión en los computadores de la Fiscalía.

Uno de los periódicos de la época informaba lo siguiente: *"Fiscalía pide investigar posible desaparición de evidencia del caso: Se trata de mails del ex gerente general que habían sido incautados por el Ministerio Público"*

Antecedentes del caso:

El fiscal del caso se contactó con la unidad especializada en la materia, donde a través de un oficio ordenó revisar si se había manipulado parte de la evidencia del caso que estaba en poder de la Fiscalía. Pues ese mismo día, el Fiscal había recibido de parte de los querellantes, una denuncia alertando la presunta desaparición de correos electrónicos

del ex gerente general, que están contenidos en un disco duro que el Ministerio Público tiene a disposición de las partes.

El juez de turno señaló en su resolución que *“en atención a lo señalado por los abogados (...) en cuanto a la falta de integridad de la evidencia en el computador del imputado, puesta a disposición de los intervinientes en un computador del Ministerio Público (...) aclárese por la requirente, emisor y destinatario de los correos (...), oficiase a la unidad especializada....a fin de que un analista de dicha unidad revise el computador disponible a los intervinientes, la evidencia aludida, constante y certifique la efectividad de lo señalado”*.

Según el documento de los querellantes, ese día "Uno de los abogados concurrió a la oficinas del Ministerio Público, con la finalidad de revisar la información incautada en el contexto de esta investigación correspondiente a los correos electrónicos que se encontraban al interior del notebook del imputado".

De acuerdo con la denuncia "al revisar la información puesta a nuestra disposición en un computador destinado especialmente para tal efecto por la fiscalía, esta parte pudo percatarse que había un número importante de correos electrónicos que habían sido revisados con anterioridad, pero que actualmente no se encontraban incorporados dentro de la evidencia revisada".

Según la denuncia, "al solicitar una explicación a la funcionaria que se encontraba presente en el lugar sobre la existencia de correos que anteriormente habían sido vistos por este interviniente al revisar la evidencia que se estaba analizando, no se obtuvo ninguna respuesta concreta ni satisfactoria". Para los querellantes hay "un indicio grave sobre la pérdida de información relevante contenida en la referida evidencia material".

Posteriormente, la Fiscalía informó que la evidencia no había desaparecido, encontrándose íntegramente disponible en poder de ese ente persecutor. La evidencia aludida se encontraba en un servidor incautado por la Fiscalía, cuyo acceso que provee de su contenido se realiza a través de un computador donde se copia la información (imagen forense).

Finalmente, este caso destaca la importancia de mantener procedimientos rigurosos en la gestión y custodia de la evidencia electrónica, garantizando su integridad y disponibilidad durante los procesos de investigación. Algunas conclusiones sobre el caso:

- Importancia de la integridad de la evidencia: La evidencia digital debe mantenerse completa y sin alteraciones para evitar dudas sobre su autenticidad.
- Transparencia en los procesos de custodia: Es fundamental que las partes intervinientes tengan claridad sobre los procedimientos de acceso y manejo de la información incautada.
- Uso adecuado de copias forenses: La creación de copias forenses asegura que la información original no se manipule durante las revisiones, garantizando su integridad.
- Comunicación clara con las partes: Las autoridades deben ofrecer explicaciones oportunas para evitar malentendidos y generar confianza en el proceso.

- Riesgo reputacional y procesal: Denuncias de pérdida de evidencia pueden comprometer la credibilidad de las instituciones encargadas de la investigación, resaltando la importancia de protocolos rigurosos.

b) Caso Práctico N° 2

En el marco de un proceso penal de alta relevancia, surgió una controversia relacionada con el manejo de información electrónica en una investigación internacional. El caso involucra la pérdida temporal de pruebas digitales críticas, lo que generó preocupación por las posibles repercusiones en la investigación y en la correcta administración de justicia. La situación pone de relieve la importancia de los controles rigurosos en el traslado y custodia de pruebas, especialmente en casos que dependen en gran medida del análisis forense de dispositivos electrónicos.

A continuación, se presentan los antecedentes relevantes que ilustran los desafíos enfrentados en la gestión de material digital en este caso particular.

La prensa nacional y extranjera informaba lo siguiente: *"Desaparecen pruebas relevantes en caso: "Discos compactos tenían información extraída de un teléfono celular y una Tablet. Peritajes estaban relacionados con uno de los sospechosos.*

Antecedentes del caso:

Cuando a mediados de año, una madre se enteró de la muerte de su hija en el extranjero, de inmediato pensó en su ex - novio. No sabía su nombre verdadero, solo su apodo, pero sabía lo suficiente como para contactarse al día siguiente con la fiscal que estaba a cargo de la investigación y nombrarlo a él como principal sospechoso del crimen de su hija.

Decía que con su hija, alumna de pregrado en una universidad estatal, y que ese año realizaba una pasantía internacional en una universidad extranjera, hablaba todos los días con ella y que no le ocultaba nada. "Por supuesto que también me habló de su ex - novio", cuenta. "De él me dijo que era obsesivo y extremadamente celoso. Ella salió con él, pero la cosa ni siquiera duró un mes. Por los celos, precisamente. Mi hija me contaba que le hacía escenas, que la llamaba a cada rato, que la esperaba a la salida de su departamento en el centro y yo le dije que terminara con él, que podía ser alguien peligroso. Y así lo hizo."

Sin embargo, por más que buscó, la policía nunca encontró nada en contra del joven, y la investigación misma cayó en un marasmo sin resultados hasta que a finales del año siguiente, cuando las cosas se precipitaron de manera espectacular.

Pocas horas después de que la policía difundiera un video donde aparecía el presunto homicida de su hija, un padre de familia llegó a un cuartel de policía acompañado de su hijo mayor. "Les vengo a entregar al asesino de la chilena", habría dicho, señalando a su hijo. Este sujeto confesó con lujo de detalles el crimen y las pruebas en su contra son inobjetables, partiendo con sus rastros de sangre que fueron encontrados en la escena del crimen.

La policía y la justicia extranjera se olvidaron del ex - novio, pero no la madre. A través de su abogado, pidió al tribunal que antes de sobreseerlo, verificara si ex – novio no había, en último término, contratado al sujeto como sicario para darle muerte a su hija. Para ello era necesario peritar celulares, tablets, computadores y lo que tuviera a mano ex - novio para enviar un mensaje. Y en eso supuestamente estaban, peritando artefactos, cuando la madre recibió una llamada de su abogado. Le dijo algo insólito: que parte de las pericias realizadas a ex - novio no estaban.

"Así mismo, como suena, no están por ninguna parte, desaparecieron", dijo el abogado desde el extranjero. "Se trataba de análisis hechos a una tablet y un celular. Los datos obtenidos estaban en unos CD y lo que faltaba era analizar dichos datos. Pero los CD no están. Se encontraban en el tribunal y de repente ya no estaban. Nadie tiene explicación de lo que pasó."

Según el abogado, se alcanzó a peritar el 70% de los aparatos electrónicos, pero falta el otro 30% de la información. Este extravío significaría un aplazamiento del juicio oral.

"Esto es alargar el dolor que sentimos como familia, alargar la agonía", dijo la madre. "Me parece demasiado extraño. ¿Cómo no se va a poder saber si este señor estuvo involucrado en la muerte de mi hija?".

Por su parte, el abogado querellante en la causa aseguró que se perdieron una tablet, entre tres a cuatro celulares y una tarjeta externa pertenecientes a ex – novio, las que son claves para probar la presunta participación del sujeto en el crimen.

Posteriormente, aparecieron las pruebas documentales y aparatos electrónicos que se habían extraviado en el marco de la investigación por el crimen de la joven estudiante chilena. El abogado defensor dio a conocer la información, pues los antecedentes habían sido enviados por error a otro tribunal. Con ello se buscaba clarificar si hubo o no un nexo entre la ex - novio de la estudiante, con el único imputado.

Finalmente, el Tribunal Oral en lo Criminal condenó al homicida, que permaneció en silencio, por considerarlo "autor penalmente responsable" del delito de homicidio doblemente agravado por alevosía y también por femicidio impropio. Este sujeto se transformó en el único imputado luego de que los resultados de las pruebas de ADN que mostraron una coincidencia del 99,99 por ciento ubicaron al acusado indudablemente en la escena del crimen.

Para concluir, podemos señalar que la pérdida temporal de pruebas digitales en este caso evidencia las vulnerabilidades existentes en los procesos de custodia y traslado de material forense. Si bien la recuperación posterior de los aparatos permitió continuar con el análisis pendiente, esta situación generó un impacto en la confianza pública hacia el proceso judicial y subrayó la necesidad de implementar controles más estrictos en la gestión de evidencia. A su vez, este incidente pone de manifiesto la importancia de asegurar la integridad y disponibilidad continua de las pruebas digitales, especialmente en investigaciones complejas que dependen de dispositivos electrónicos para esclarecer los hechos. Asimismo, destaca la necesidad de procedimientos más claros de coordinación

entre las distintas jurisdicciones, para evitar errores administrativos que puedan afectar el curso de la justicia. Algunas conclusiones sobre el caso:

- Importancia de la custodia adecuada de evidencia digital: El manejo descuidado de pruebas digitales puede poner en riesgo investigaciones completas. Es fundamental contar con procedimientos claros para la custodia y el traslado de material forense.
 - Necesidad de protocolos de gestión interjurisdiccional: El envío erróneo de pruebas entre tribunales resalta la importancia de una coordinación eficiente entre distintas jurisdicciones, especialmente en casos internacionales.
 - Impacto en la confianza pública y en la justicia: La pérdida temporal de información afecta la percepción pública sobre la integridad del proceso judicial, lo que subraya la necesidad de transparencia y rigor en cada etapa.
 - Controles adicionales en el manejo de dispositivos electrónicos: Dado que gran parte de la información digital se basa en dispositivos electrónicos, es necesario desarrollar competencias avanzadas en informática forense y asegurar que cada etapa del análisis se complete sin interrupciones.
 - Redundancia y trazabilidad de las pruebas: Este caso pone de manifiesto la importancia de contar con copias de respaldo y registros detallados del traslado de evidencia, para prevenir errores y facilitar su localización inmediata si surgen problemas.
- Análisis comparativo caso 1 y 2

En términos generales, ambos casos exponen desafíos en la gestión de evidencia digital y las consecuencias de errores en su custodia. Sin embargo, presentan diferencias relevantes que afectan tanto el desarrollo del proceso judicial como la percepción pública de las instituciones. ¿por qué ante similares circunstancias - pérdida de evidencia digital- se habla en la primera noticia de “desaparición de evidencia” y, en la otra de “desaparición de pruebas”? Sin duda que existe una distinción fundamental entre los términos "evidencia" y "pruebas", por lo que es clave entender las diferencias entre ambos contextos.

El siguiente análisis compara estas dos situaciones que muestran la diferencia entre “evidencia” y “prueba” en distintos momentos procesales: una fase investigativa preliminar y un juicio oral próximo. A continuación, se detalla cómo estos términos se utilizan en cada caso y cómo impactan en el proceso judicial.

1. Naturaleza conceptual

- Evidencia: Cualquier información recopilada durante una investigación con el potencial de convertirse en prueba. Su valor depende de una adecuada preservación y custodia hasta que pueda ser utilizada en juicio.

- Pruebas: Son evidencias que, una vez validadas, se presentan formalmente en juicio para demostrar hechos específicos. Las pruebas adquieren un estatus procesal superior al sustentar directamente la decisión del tribunal.

2. Etapa procesal

Caso 1: Se utiliza el término "evidencia" porque el material se encuentra en una fase preliminar de investigación, por lo que aún no ha sido formalmente utilizada como prueba ante el tribunal.

Caso 2: El término "pruebas" es más adecuado, porque hace referencia a información digital ya sometida a análisis pericial, para sustentar hechos concretos y acusaciones formales, a ser utilizadas en un juicio oral próximo, destacando su relevancia procesal. La pérdida temporal de evidencia en esta fase puede impactar gravemente el proceso.

3. Contexto

Caso 1: La controversia surge en una fase investigativa temprana, cuestionando la integridad de correos electrónicos incautados y el acceso a estos por las partes intervinientes.

Caso 2: La polémica ocurre durante un proceso pericial avanzado, cercano al juicio oral, lo que afectó directamente el desarrollo del proceso judicial.

9.2. Cuando el auditor está en estrados³⁶

El siguiente caso es real y ocurrió en el extranjero, marcando un antes y un después en la forma en que los auditores forenses (profesionales de la auditoría, al fin y al cabo) deben presentar sus hallazgos.

1. Antecedentes preliminares del caso

Un regulador financiero independiente había iniciado la apertura de un proceso legal contra los exdirectores de una prestigiosa compañía de telecomunicaciones internacional, cuyas alegaciones se fundaban en la contravención de la ley de sociedades anónimas de ese país. Dicha ley exige que los directores actúen con un grado razonable de debido cuidado y diligencia. Ante este contexto, el regulador prohibió a los demandados administrar sociedades, ordenándoles a pagar una indemnización de aproximadamente 92 millones de dólares estadounidenses.

El juicio comenzó ante el Tribunal Supremo a fines de 2004. Durante el curso del juicio, que duró 232 días, los demandados se opusieron a que ese organismo regulador presentara un informe pericial de auditoría forense preparado por un auditor perteneciente a una firma líder en auditoría (Big Four). El informe se refería a la situación financiera del Grupo de Telecomunicaciones, las razones de la situación financiera del holding, la

³⁶ DE YOUNG, NICK, 2005, "Expert forensic accounting evidence: when is it admissible?", Litigation and Dispute Resolution Insights, CLAYTON UTZ.

naturaleza de la información de la administración al directorio de esa compañía y la reducción del patrimonio neto del grupo, siendo esta última cuestión relevante para la cuantificación de la reclamación de indemnización.

La parte demandada objetó el informe del auditor forense. La objeción se basó en el hecho de que el auditor y otros miembros de la firma de auditoría estaban estrechamente implicados en el proceso de investigación que se llevó desde el inicio del procedimiento judicial. Posteriormente, se tomó la decisión de que el auditor prestara declaración en el juicio. A partir de ese momento, no volvió a desempeñar ningún rol activo en la preparación del caso del organismo regulador, pero otras personas que habían trabajado con él continuaron desempeñando ese rol y le ayudaron en la preparación del informe. El auditor elaboró un borrador de informe que se basaba en una amplia gama de evidencias. Sin embargo, en un momento dado se le pidió que excluyera gran parte de ellas (presumiblemente porque no podían probarse) con los efectos de encarar lo que sería su informe final.

En primera instancia, el juez dictaminó que el informe del auditor era inadmisibile porque no identificaba la base fáctica "verdadera" del informe, como lo exigen los principios de la prueba pericial. Su valor probatorio se vio sustancialmente superado por el peligro de que las pruebas pudieran ser injustamente perjudiciales, engañosas o confusas, o que dieran lugar a una pérdida de tiempo indebida.

Ante esto, la parte demandante apeló. En efecto, el Tribunal de Apelación anuló la decisión del juez en primera instancia sobre la base de que los estándares de prueba pericial de ese Estado no exigían que un informe revelara la verdadera base fáctica de los informes evacuados, bastando con que revelaran los hechos y el proceso de razonamiento que, según el experto, justificaban sus opiniones expresadas. Asimismo, el tribunal sostuvo que el juez debió, antes, realizar un análisis sistemático del valor probatorio de la evidencia del auditor.

En la última decisión del juez, en vista de la decisión del Tribunal de Apelación, este llevó a cabo un análisis párrafo por párrafo del informe del auditor en virtud de las facultades que la ley le otorgaba. El resultado fue que su Señoría rechazó más partes del informe de lo que se esperaba.

2. El juez rechazó gran parte de la evidencia del auditor porque:

- El informe no era más que resúmenes descriptivos de documentos.
- Los defectos en el proceso de razonamiento o en los hechos subyacentes significaban que la evidencia tenía un valor probatorio bajo y que era probable que ese valor probatorio se viera sustancialmente superado por el peligro de que las pruebas pudieran ser injustamente perjudiciales, engañosas o confusas, o que dieran lugar a una pérdida de tiempo indebida.
- En el caso de los cuadros informativos, las pruebas practicadas requerían poca pericia contable y podían proporcionarse con la misma facilidad que un documento basado en las pruebas documentales.

- La opinión forense no se basaba en el conocimiento especializado del auditor y era simplemente un argumento en apoyo del regulador.

Sin embargo, el juez permitió algunas piezas de pruebas basado en:

- En el caso de la construcción de tablas, la selección del material y los cálculos matemáticos requerían cierta habilidad de contabilidad forense; o el auditor había reunido la información de una manera conveniente y útil.
- Hubo una ilación racional en la argumentación entre los documentos identificados y las conclusiones del auditor.

3. Hay dos cuestiones importantes que se plantean en este caso:

A menudo es necesario obtener asesoramiento experto en auditoría forense de forma anticipada para determinar si se debe iniciar un procedimiento judicial y, en caso afirmativo, para definir el alcance de dicho procedimiento. En este caso, el demandante podría tener dos opciones con respecto a la prueba pericial en el proceso: en primer lugar, intentar "poner en cuarentena" al perito antes de la presentación de la prueba que puede demostrarse en un juicio; o, en segundo lugar, contratar a un nuevo perito al que solo se le dé acceso a las pruebas que puedan ser demostradas en un juicio.

Los auditores forenses deben limitar sus pruebas a asuntos dentro de su área de especialización. Esta regla se vuelve difícil de aplicar cuando se consideran tablas, esquemas o gráficos que contienen información extraída de diversas fuentes. Estas pruebas son cada vez más importantes dada la complejidad de la mayoría de las transacciones comerciales y negocios actuales. El juez resumió los principios que deben aplicarse en estas circunstancias de la siguiente manera:

"Un auditor forense puede aportar las pruebas admisibles que impliquen extraer y condensar, a partir de una gran cantidad de documentos, la información que considere importante, incluso cuando los documentos sean pruebas y, en teoría, el abogado y el tribunal podrían extraer la misma información sin la asistencia del perito. Esas pruebas deben distinguirse de las pruebas que no son más que la reproducción de pruebas fácilmente accesibles en documentos que se explican por sí mismos (con una explicación del abogado en las comunicaciones)".

Ahora, el caso analizado resalta la importancia de la rigurosidad en la preparación y presentación de pruebas periciales en auditoría forense. Las decisiones judiciales evidencian que los informes periciales deben ir más allá de la simple recopilación de datos, incorporando un proceso de razonamiento claro y fundamentado que aporte un valor probatorio significativo. La admisibilidad de las pruebas depende no solo de su contenido, sino también de la capacidad del auditor para limitarse a su área de especialización y presentar la información de manera útil y comprensible para el proceso judicial.

Asimismo, se destaca que la preparación de pruebas debe realizarse con anticipación para definir su alcance y asegurar su validez. El intento de "poner en cuarentena" al perito o de limitar su acceso a determinadas pruebas refleja la necesidad de gestionar

adecuadamente el rol del auditor durante el juicio. Las pruebas deben ser cuidadosamente seleccionadas para evitar que su presentación se convierta en una repetición innecesaria de documentos que ya pueden ser explicados por los abogados o el tribunal.

En conclusión, este caso deja en evidencia que la adecuada preparación de las pruebas periciales desde etapas tempranas es crucial. El rechazo de una prueba en juicio puede tener consecuencias graves, limitando la posibilidad de presentar evidencia alternativa. Por ello, es fundamental que los auditores forenses actúen con precisión técnica, dentro de su área de conocimiento, y aporten información que realmente agregue valor al proceso judicial.

X. APÉNDICE: Principios generales para la evidencia digital [CONFERENCE OF INTERNATIONAL INVESTIGATORS, CII 2021]

El aspecto más crucial de las investigaciones digitales es garantizar la confiabilidad de la evidencia digital. En la era digital, la mayoría (–si no todas–) las investigaciones involucran evidencia digital, y todos los investigadores deben estar familiarizados con las mejores prácticas actuales para el manejo de evidencia digital. Estos principios se centrarán en la integridad, confidencialidad y autenticidad de la evidencia digital.

Estos principios generales deben utilizarse en el marco de las políticas de cada organización y en el ejercicio del criterio y experiencia profesional de una oficina de investigación.

- Autenticidad, integridad y confidencialidad
 1. Como resultado, es necesaria una consideración especial para establecer la autenticidad, proteger la integridad y mantener la confidencialidad de la evidencia digital. Estas consideraciones incluyen:
 - Garantizar que la recopilación de evidencia digital esté debidamente autorizada y realizada de conformidad con las políticas de la organización.
 - Documentar el levantamiento de datos y conservar la documentación para su posterior revisión.
 - No alterar la evidencia digital, a menos que sea necesario, y solo por personas capacitadas para ello.
 - Documentar todas las interacciones con la evidencia.
 - Establecer una cadena de custodia lo antes posible.
 - Realizar copias de seguridad de la evidencia digital y trabajar únicamente con copias.
 - Garantizar que la evidencia y todas las copias se almacenen, transporten y eliminen de forma segura.
- Identificación
 2. Al comienzo de una investigación, se deben identificar y preservar todas las posibles fuentes de evidencia digital potencialmente relevantes para la investigación. La evidencia digital puede ser de naturaleza temporal, y el tiempo es un factor crítico.
 3. Las posibles fuentes de evidencia digital incluyen computadoras, dispositivos móviles, medios de almacenamiento externos, servidores de red, almacenamiento en la nube e Internet.
 4. Para limitar los volúmenes de datos y reducir la posibilidad de intrusión colateral, se debe considerar cuidadosamente la proporcionalidad y relevancia de la evidencia digital. La recopilación de la evidencia digital y/o el alcance del examen forense digital deben reflejar esto.

- Recopilación
- 5. Para garantizar la confiabilidad de la evidencia digital, es fundamental no modificarla. Cualquier acción que pueda modificar la evidencia solo debe ser realizada por una persona especialmente capacitada, y todos los pasos deben documentarse.
- 6. Las interacciones con dispositivos activos (encendidos) deben mantenerse al mínimo, ya que es probable que modifiquen y sobrescriban datos potencialmente relevantes. Los dispositivos móviles deben desconectarse de todas las redes para evitar el borrado remoto.
- 7. Si el dispositivo está encendido, se debe apagar lo antes posible. Sin embargo, si los datos “en vivo” pueden ser de interés, si el cifrado está habilitado o no se puede obtener una contraseña para desbloquear un dispositivo móvil, el dispositivo debe mantenerse encendido, y se debe consultar a un experto forense digital.
- 8. Al realizar un apagado adecuado, normalmente se realizan varias escrituras en el dispositivo de almacenamiento interno. Para evitar esto, se puede apagar un dispositivo quitando el cable de alimentación y/o las baterías.
- 9. Como las unidades de almacenamiento interno son cada vez más difíciles de extraer, puede resultar más práctico recoger el dispositivo y el cable de alimentación.
- 10. En circunstancias en las que la recolección física no sea factible, se puede adquirir una computadora a través de una red utilizando herramientas de recolección remota.
- Cadena de Custodia
- 11. La cadena de custodia de la evidencia digital es la documentación cronológica de su manejo desde el momento de su recolección hasta su disposición en juicio. La cadena de custodia puede consistir en formularios en papel firmados, fotografías, notas del investigador, informes de exámenes, registros generados automáticamente y hashes forenses.
- 12. La cadena de custodia debe identificar de manera única la evidencia. Las computadoras, teléfonos y otros medios de almacenamiento se pueden identificar registrando el nombre del fabricante, el número de modelo y el número de serie. Si no existe un identificador único, la evidencia se puede etiquetar o codificar con barras para ese propósito específico.
- 13. Las pruebas digitales, como correos electrónicos, documentos digitales, archivos multimedia o capturas de sitios web, pueden identificarse por cómo, cuándo y de quién se recibieron, o por cómo, cuándo y dónde se recogieron.

14. Como mínimo, la cadena de custodia debe documentar lo siguiente:

- La persona que recoge o recibe la evidencia.
- La fuente de la evidencia.
- Fecha y hora, incluida la información de zona horaria cuando corresponda.
- Identificadores únicos.
- Cómo se recopiló la evidencia, incluidas las herramientas y métodos utilizados.
- Cualquier documentación adicional que requiera la organización.

- “Hashes” Forenses

15. Los hashes forenses, a veces denominados huellas digitales, son valores que identifican de forma única la evidencia digital. Los hashes forenses se utilizan para verificar la integridad de todo tipo de evidencia digital y para verificar que las copias sean idénticas al original.

16. Los hashes forenses se calculan utilizando funciones matemáticas, más comúnmente los algoritmos Message Digest (MD5) y Secure Hash (SHA), entre Otros.

- Examen de la evidencia digital

17. El examen de la evidencia digital solo debe realizarse en copias de trabajo.

18. Las computadoras, los dispositivos móviles y los medios de almacenamiento externos originales solo deben ser examinados por examinadores forenses digitales debidamente capacitados. Navegar por una computadora/dispositivo móvil o conectar un dispositivo de almacenamiento externo para obtener una vista previa de su contenido podría comprometer la integridad de la evidencia digital y debe evitarse.

19. Al utilizar herramientas de análisis que emplean búsquedas por palabras clave, se debe garantizar que se utilice una herramienta de reconocimiento óptico de caracteres (OCR) para convertir todo el contenido que no permite búsquedas antes de la indexación, o que los documentos no accesibles por búsqueda, como los escaneados, se revisen manualmente.

20. Por razones de seguridad de los datos y de la red, se recomienda que las pruebas digitales se examinen en una computadora dedicada, aislada de todas las redes.

21. Debe evitarse el uso de computadoras personales o medios de almacenamiento para almacenar o visualizar evidencia digital, así como el uso de cuentas personales para buscar o descargar información de Internet.

22. Todas las herramientas y métodos utilizados para el examen de pruebas digitales deben documentarse.

- Autenticación

23. Los investigadores deben ser conscientes de que la evidencia digital puede manipularse fácilmente sin dejar rastro.
24. Se recomienda autenticar la evidencia digital proporcionada por terceros, como denunciantes o testigos. Preferentemente, la evidencia debe recopilarse directamente de su entorno nativo, por ejemplo, una computadora, un dispositivo móvil, una cuenta de redes sociales o un sitio web.
25. Si no es posible recopilar la evidencia de la fuente original (por ejemplo, cuando un testigo no está dispuesto a entregar su dispositivo personal para la adquisición forense digital), el investigador debe intentar verificar la evidencia confirmando su existencia en el dispositivo original o en la cuenta en línea.
26. Los metadatos de documentos que no se examinen en su entorno nativo (el dispositivo utilizado para crearlos o modificarlos) no deben tomarse al pie de la letra.

- Almacenamiento, Transporte y Eliminación

27. Para mantener la confidencialidad, el acceso a toda la evidencia digital (incluidas las copias de trabajo) debe limitarse únicamente al personal autorizado.
28. Si la evidencia se almacena en servidores en red o se transmite a través de redes, se debe utilizar un control de acceso estricto y transmisiones cifradas. Los dispositivos de almacenamiento portátiles utilizados para transportar pruebas deben estar cifrados.
29. La evidencia digital debe transportarse en embalajes adecuados y protegerse de temperaturas extremas, humedad, golpes físicos, electricidad estática y campos magnéticos.
30. Cada computadora y dispositivo de almacenamiento utilizado para almacenar o visualizar evidencia digital debe limpiarse adecuadamente antes de ser transferido a otro usuario o reciclado.

- Directrices de Publicación e Implementación

31. Estos principios generales han sido avalados por la CII. Cualquier organización puede hacer referencia a estos principios generales en sus propias políticas o publicarlos de acuerdo con sus directrices. Además de estos principios generales, en julio de 2020, el Grupo de Trabajo Interinstitucional de Investigaciones Digitales (DIG) publicó Directrices sobre Evidencia Digital, que pueden utilizarse como orientación adicional no vinculante.

XI. BIBLIOGRAFÍA

- ACADEMIA JUDICIAL DE CHILE, 2022, “Valoración Probatoria: Exigencias Legales, Jurisprudenciales y Doctrinales”, Juan S. Vera Sánchez, Colección Materiales Docentes 51.
- AGUIRREZABAL, MAITE & FLORES, JUAN C., 2021, “La prueba como Elemento Esencial del Debido Procedimiento Administrativo”, REVISTA DE DERECHO ADMINISTRATIVO ECONÓMICO, REDAE, Nº 33, Facultad de Derecho, Pontificia Universidad Católica de Chile.
- ÁLVAREZ SAAVEDRA, FÉLIX, 2008, “Diccionario de Criminalística: Los secretos de las Investigaciones de la Policía Científica”, Editorial Planeta S.A., España.
- ALVIN A. ARENS (†), RANDAL J. ELDER, MARK S. BEASLEY AND CHRIS E. HOGAN, 2017, “Auditing and Assurance Services: An Integrated Approach”, Sixteenth Edition, Global version, Pearson Education.
- ARROYO, JENNIFER, 2014, “Similitudes y Diferencias entre la Evidencia de Auditoría y la Prueba en el Procedimiento Judicial o Administrativo”, Revista Nacional de administración, Vol. 5 (2).
- BEASLEY, MARK S., CARCELLO, JOSEPH, HERMANSON, DANA & NEAL.TERRY, 2013, “An Analysis of Alleged Auditor Deficiencies in SEC Fraud Investigations: 1998–2010”, Estados Unidos. Funding for this research project was provided by the CENTRE FOR AUDIT QUALITY.
- CARDOZO BRUM, MYRIAM, 2021, “Evidencia: conceptos y usos en la evaluación de políticas y programas públicos”, Iztapalapa. Revista de ciencias sociales y humanidades, México, <https://doi.org/10.28928/ri/902021/aot3/cardozobrumm> [Último acceso: Junio del 2024].
- CASEY, EOGHAN, 2011, “Digital evidence and computer crime: Forensic science, computers and the internet”, 3rd Edition, Academic Press, Estados Unidos.
- CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO, Documentos Técnicos disponibles en: <https://www.auditoriainternadegobierno.gob.cl/documentos-tecnicos/>
- CALDANA, DANIELLA, CORREA, RICARDO & PONCE, HECTOR, 2007, “Competencias de los auditores gubernamentales para la obtención de evidencia electrónica de auditoría”, Contaduría y Administración, (223), pp. 9-31, Universidad Nacional Autónoma de México.
- DAMIAN MANFREDI, MARIANO, 2023, “Introducción a la evidencia digital”, MINISTERIO PÚBLICO Fiscal de la Ciudad Autónoma de Buenos Aires - MPF CABA.
- DE YOUNG, NICK, 2005, “Expert forensic accounting evidence: when is it admissible?”, Litigation and Dispute Resolution Insights, CLAYTON UTZ.

- DROGHETTI FUENTES, PIA ALEJANDRA & PÉREZ JIMÉNEZ, MARIAJOSÉ, 2017, “La Actividad Probatoria en el Derecho Administrativo Sancionador a la luz de la Ley de Bases de los Procedimientos Administrativos”, FACULTAD DE DERECHO, DEPARTAMENTO DE DERECHO PÚBLICO, UNIVERSIDAD DE CHILE (Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales).
- INTERNATIONAL AUDITING AND ASSURANCE STANDARDS BOARD, IAASB, 2023-4, “Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements”, Vol. 1, IFAC.
- INSTITUTO DE AUDITORES INTERNOS, IIA, 2024, “Normas Globales de Auditoría Interna”:
<https://www.theiia.org/globalassets/site/standards/editable-versions/global-internal-audit-standards-spanish.pdf>
- JIMÉNEZ BARAHONA, MAGDALENA *et al*, 2004, “Aspectos Generales de la Prueba y los Medios de Prueba”, Material Docente, Escuela de Derecho, Universidad de Chile, U Cursos.
- KÄVRESTAD, JOAKIM, 2020, “Fundamentals of Digital Forensics: Theory, Methods, and Real-Life, Applications”, Second Edition, Springer Nature Switzerland.
- KRUSE, WARREN G. & HEISER, JAY G., 2002, “Computer forensics: incident response essentials”, Addison-Wesley, Estados Unidos.
- LARROUCAU TORRES, JORGE, 2012, en EXCMA. CORTE SUPREMA, uno de abril de 1974, REVISTA DE DERECHO Y JURISPRUDENCIA, Tomo 68 (1971), Sección 1ª, p.76, citado en Rioseco (1995) t.II N°694 p. 378.),
- LIN, XIAODONG, 2018, “Introductory Computer Forensics: A Hands-on Practical Approach”, Springer Nature Switzerland.
- MAUTZ, R.K. & SHARAF, HUSSEIN A., 1961, “The Philosophy of Auditing”, 18 Edition (1997), American Accounting Association, Estados Unidos.
- MANS PUIGARNAU, JAIME, 2015, “Lógica para Juristas”, Bosch Casa Editorial S.A., Barcelona, 1978, citado por HERNANDO BERMÚDEZ GÓMEZ, Parte II, Evidencia en Auditoría, “Auditoría y Control”, Pontificia Universidad Javeriana, Colombia.
- MENESES PACHECO, CLAUDIO, 2008. “fuentes de prueba y medios de prueba en el proceso civil”, Revista Ius et Praxis, Vol. 14(2), <https://dx.doi.org/10.4067/S0718-00122008000200003> [Último acceso: Junio del 2024].
- NINO-MORIS, CHRISTIAN, 2020, “Tribunales de justicia y evidencia digital: una oportunidad que se vislumbra por Covid-19”, <https://www.elmercurio.com/legal/movil/detalle.aspx?Id=908836&Path=/OD/DE/> [Último acceso: Junio 2024].

- 2023, “La Concepción del Fraude en la Profesión del Auditor y Algunas Implicancias Jurídicas en el Derecho Penal Económico, y su Impacto en la Evacuación del Informe Pericial Contable”, tesina como requisito para optar al grado de Magíster en Derecho Penal Económico y de la Empresa, Universidad San Sebastián (obra inédita no publicable).

PARRONDO, LUZ & AMAT, ORIOL (Editors), 2024, “Comprehensive red flag model for accounting fraud detection using qualitative and quantitative variables”, Research Handbook on Financial Accounting, Edward Elgar Publishing.

PODER JUDICIAL, EXCMA. CORTE SUPREMA, Sentencia del seis de septiembre de 2016, Causa ROL 9086-2015, considerando Séptimo.

- EXCMA. CORTE SUPREMA, Sentencia del cuatro de agosto de 2014, Causa ROL 15256-2014, considerando Quinto.

FORENSIC EXAMINATION OF DIGITAL EVIDENCE: A GUIDE FOR LAW ENFORCEMENT, 2004, US Department of Justice, Office of Justice Programs, National Institute of Justice; Counter Fraud Authority.

VÁSQUEZ, CARMEN, 2015, “De la prueba científica a la prueba pericial”, Marcial Pons, Ediciones Jurídicas y Sociales, España.



Ministerio
Secretaría
General de la
Presidencia

Gobierno de Chile



DOCUMENTO TÉCNICO N° 130

Versión 0.1

ASPECTOS FUNDAMENTALES SOBRE LA EVIDENCIA DE AUDITORÍA

Este documento técnico proporciona una guía integral sobre la evidencia de auditoría en el contexto de la auditoría interna del sector público chileno. A través de un análisis detallado de los principios y normas que rigen la obtención y evaluación de la evidencia, incluyendo las Normas Globales de Auditoría Interna del IIA, así como los estándares, leyes y mejores prácticas aplicables en el ámbito de la auditoría, se busca equipar a los auditores con conocimientos para realizar su labor de manera efectiva y objetiva.

