CONGRESO DE

TRIBUNALES DE CUENTAS, ÓRGANOS Y ORGANISMOS DE CONTROL.

PROVINCIA DE SAN LUIS.

NOVIEMBRE 2022.

TEMA 1: TRANSFORMACIÓN DIGITAL

Aplicación de nuevas herramientas tecnológicas en los Procesos de Control

Cadena de custodia de evidencias digitales

Integrantes: **Cdra. Adriana Agüero**
Ing. Roxana Piottante

TRIBUNAL DE CUENTAS DE MENDOZA

"El Tribunal de Cuentas de la Provincia de Mendoza, ha tomado conocimiento de la presentación del presente trabajo para el XXVI Congreso Nacional de Tribunales de Cuentas, Órganos y Organismos Públicos de Control Externo, según Acuerdo Nº5507 de fecha 24 de agosto de 2022"

ÍNDICE

I. RESUMEN:

Desde el año 2019 son cada vez más y más los organismos que se vuelcan a la documentación digital, dejando de lado el soporte papel. Con la pandemia se ha elevado exponencialmente la velocidad de cambio y la digitalización de los procesos, haciendo que tanto los organismos gubernamentales como también la gran mayoría de los ciudadanos se sientan motivados al uso de medios de pagos digitales, completar fichas electrónicas de datos, iniciar un trámite vía web, etc.

Por lo que las evidencias en el proceso de auditoría han cambiado su soporte siendo hoy digitales, pero además son: sensibles, de fácil cambio de estado, de posible manipulación y difícil validez probatoria.

El nuevo desafío de los órganos de control es utilizar herramientas para proteger la evidencia de auditoría, de manera de cumplir con el requisito de validez durante todo el proceso y ante la Justicia.

II. METODOLOGIA DE INVESTIGACION

Se plantea, entonces, la necesidad de adaptar algunas formas de trabajo que venían realizándose con la evidencia documental en soporte papel a una que tome en cuenta que la evidencia es digital, donde hay que considerar especialmente: la forma de obtención, recopilación y resguardo de pruebas digitales halladas en el proceso de auditoría como así también analizar la suficiencia y validez de las presentadas por los responsables en el juicio de cuentas.

Para ello se efectuó entrevista a las autoridades directivas del Tribunal de Cuentas. Asimismo, se realizó un análisis cualitativo de la realidad del contexto y del organismo de control externo de la Provincia de Mendoza de los últimos dos años, a través de la lectura de las instrucciones de trabajo y la normativa provincial, nacional e internacional en la materia abordada y relacionada.

III. DESARROLLO

1. Objetivo

Establecer una metodología o protocolo para asegurar la integridad de la información que constituye la evidencia digital del informe del auditor. Asimismo, se aspira a asegurar los papeles de trabajo digitales del auditor.

La finalidad es evitar que con, o sin intención, las pruebas o evidencias de auditoría sean modificadas.

2. Análisis de contexto institucional

El Honorable Tribunal de Cuentas de Mendoza, en adelante HTC, tiene su mandato establecido por la Constitución Provincial.

Art 181 Constitución Provincial "*Habrá un Tribunal de Cuentas con jurisdicción en toda la Provincia y con poder bastante para aprobar o desaprobar la percepción e inversión de caudales públicos hechas por todos los funcionarios, empleados y administradores de la Provincia.*"

Su ley reglamentaria Ley N.º 9292, en su Art. N.º 3 habla de su jurisdicción y competencia:

"Art. 3º Las cuentas rendidas sólo podrán ser definitivamente aprobadas o desaprobados por el Tribunal de Cuentas y en consecuencia, su fallo será el único que exonere de todo cargo a los cuentadantes, salvo el pronunciamiento de la Suprema Corte, en los caos de revisión judicial plena prevista por el artículo 57, siguientes y concordantes de esta ley y sin perjuicio de la prescripción contemplada en el Art. 182 de la Constitución Provincial."

Sus principales procesos son el de Planificación, Fiscalización, Juicio de Cuentas y Asesoramiento e informes especiales.

Los procedimientos de auditoría se establecen dentro de Instrucciones de Trabajo los cuales podemos encontrar en el Manual de Auditoría del Tribunal.

3. Análisis del ambiente y contexto actual

La evidencia digital es un tema muy estudiado y abordado por la Justicia Penal y especialistas informáticos forenses. Hoy la extensiva utilización de los dispositivos tecnológicos penetra en la ciudadanía y en las administraciones de los estados, como una manera de realizar las actividades, transacciones, documentar procesos y registrar operaciones.

En este mundo, con un entorno VICA[1] (VUCA por sus siglas en ingles Volatilidad, Incertidumbre, Complejidad y Ambigüedad) el ritmo de los cambios tecnológicos y la digitalización de los procesos es vertiginoso empujando a las instituciones a adaptarse a las nuevas necesidades de la población y haciendo uso por ejemplo de medios de pagos digitales (billeteras virtuales), completando fichas electrónicas de datos, iniciando y posibilitando los trámites vía web, guardando respaldo documental de operaciones en soportes electrónicos.

Este tema, no escapa de la labor diaria que realizamos en el Tribunal de Cuentas, donde los auditores contadores emiten una opinión de la razonabilidad de los estados contables en su conjunto, siendo el respaldo documental digital.

Esto motiva y hace necesario estudiar distintos medios para lograr que la prueba documental o evidencia de auditoría llegue al juicio de cuentas, y si es el caso ante la misma Suprema Corte de Justicia de la Provincia de Mendoza, de manera protegida, para que sea plenamente válida.

Nos preguntamos: ¿Cómo protegemos la evidencia ante posibles manipulaciones?

Consideramos que la respuesta se encuentra en las guías de buenas prácticas como son la ISO 27037 y el Convenio de Budapest suscripto por varios países entre los cuales se encuentra la República Argentina.

4. Alcance del trabajo y marco conceptual

4.1. Alcance

Establecer un procedimiento con lineamientos generales que permitan proteger o preservar la documentación relevante en formato digital para garantizar su validez, tanto

[1] **VUCA** es un acrónimo utilizado para describir o reflejar la **volatilidad**, **incertidumbre** (*uncertainty* en inglés), **complejidad** y **ambigüedad** de condiciones y situaciones. https://es.wikipedia.org/wiki/VUCA , extraído 08/08/2022.

en el proceso de Juicio de Cuentas, como para la eventual formulación de una denuncia ante la Justicia.

Establecer procedimientos generales para la cadena de custodia de la evidencia no firmada digitalmente por el responsable de su producción.

Por lo expuesto, la cadena de custodia no incluye a la documentación que cumple con el Art. 11 de la 25506 de firma digital, dado que son consideradas originales y válidos. *"ARTÍCULO 11. — Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación."*

Es importante distinguir el valor probatorio de la evidencia digital en soporte electrónico cuya primera generación ha sido en papel, para la norma nacional y la norma provincial.

El decreto nacional N.º 1131/2016 refiere respecto lo siguiente:

"ARTICULO 1º-Los documentos y expedientes generados en soporte electrónico y los reproducidos en soporte electrónico a partir de originales de primera generación en cualquier otro soporte, digitalizados de acuerdo al procedimientos que establezca al SECRETARIA DE MODERNIZACION ADMINISTRATIVA del MINISTERIO DE MODERNIZACION, son considerados originales y tienen idéntica eficacia y valor probatorio que sus equivalentes en soporte papel, en los términos del artículo 293 y concordantes del Código Civil y Comercial de la Nación.

ARTÍCULO 2º - Los documentos y expedientes producidos en primera generación en soporte papel deberán ser digitalizados siguiendo el procedimiento que fije la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA y perderán su condición jurídica de original, pudiendo ser destruidos y otorgarse a los mismos el destino que la autoridad competente determine."

En el caso del HTC, el artículo 5 del Acuerdo N.º 6.569 establece los requisitos de las actuaciones administrativas electrónicas;

***"Artículo 5º:** Las actuaciones administrativas electrónica, deben cumplircon los siguientes requisitos mínimos:*

a) Los establecidos por la Ley Provincial de Procedimiento Administrativo N.º 9003,

o las que resulten de aplicación para las personas jurídicas privadas respecto a ordenamiento de expedientes.

b) Al momento de incorporar documentación al Sistema de Gestión Documental Electrónica, se debe priorizar los documentos originales en formato digital.

c) Las actuaciones que se encuentren en soporte papel incorporadas al Sistema de Gestión Documental Electrónica, a través de escaneo, no podrán destruirse y deberán estar a disposición de este Tribunal de Cuentas,ordenados y referenciado a los expedientes donde se incorporaron las mismas.

En la digitalización del soporte papel, el contenido debe ser: integro, con las características de legibilidad, claridad y adecuada resolución gráfica, con la finalidad de una correcta visualización y accesibilidad.

d) Estar firmadas conforme normativa vigente."

4.2. Definiciones

Evidencia digital*:* La guía de obtención, preservación y tratamiento digital del Ministerio Público Fiscal de la República Argentina cita como definición de evidencia digital a: *«Conjunto de datos e información, relevantes para una investigación, que se encuentra almacenada o es transmitida por una computadora o dispositivo electrónico»*[2]

Para el "Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Procesos de recolección de pruebas en ciberdelitos" del Ministerio de Seguridad de la Nación, **evidencia digital** es: *"Información y datos de valor en una investigación que se encuentra almacenada, es recibida o transmitida por un dispositivo electrónico. Dicha prueba se adquiere cuando se secuestra y asegura para su posterior examen. Normalmente las pruebas consisten en archivos digitales de texto, vídeo o imagen, que se localizan en ordenadores y todo tipo de dispositivos*

[2] Guía de obtención, preservación y tratamiento de evidencia digital. Resolución 756/16 de fecha 31 de marzo de 2016. Procuración General de la Nación. Extraída de: https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf

electrónicos."[3] Esta definición no es aplicable a las tareas que realiza el órgano de control externo.

El Art. 6 de la ley 25506 define documento digital. *"Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura."* [4]

Hash: se refiere a una función o método para generar claves o llaves que representen de manera unívoca a un documento, registro, archivo, etc.

Cadena de custodia: Es la forma metódica de obtención, recopilación y resguardo de la evidencia digital que no posee la firma digital y/o electrónica.

Norma ISO/IEC 27037: "*Guía para la identificación, recolección, adquisición y preservación de evidencias digitales": "Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos, para que puedan ser utilizadas con valor probatorio."*

4.3. Características de las pruebas

Del estudio de diferentes fuentes de información, se verifica que se coincide en que; para poder ser tomada como medio de prueba potencial, la evidencia digital debe reunir las siguientes propiedades:

- Relevante o significativa
- Confiable y Auditable
- Suficiente

4.4. Cadena de custodia: Etapas del proceso

[3] Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Procesos de recolección de pruebas en ciberdelitos. Resol 234/2016 Ministerio de Seguridad de 7 de junio de 2016.Extraida de: https://www.boletinoficial.gob.ar/detalleAviso/primera/146717/20160614?busqueda=1

[4] Ley 25506 Firma Digital. Congreso de la Nación Argentina 14/11/2001. BO 14/12/2001.

Las evidencias digitales, tienen como característica, ser sensibles, de fácil cambio de estado, de posible manipulación y por eso son consideradas como de difícil validez probatoria. Debido a esto, es el rigor en cuanto a los procedimientos que se deben acatar para poder tomarlas como válidas para un juicio.

Este rigor procedimental, ha sido, y sigue siendo estudiado, por los organismos internacionales que luchan contra la corrupción y el ciberdelito. La norma ISO/IEC 27037 establece para el tratamiento genérico de las evidencias tres procesos: Identificación, Adquisición y Conservación.[5]

En nuestra propuesta de trabajo dividimos las tareas en dos procesos, a los cuales denominamos: obtención y resguardo.

Se entiende, como **obtención** de la evidencia, al momento en el que el auditor identifica y recopila la información digital para poder tomarlo como prueba en el Juicio de Cuentas, en los distintos informes que realiza el Auditor contador y los cuales son soporte del Fallo del Tribunal de Cuentas.

En este sentido, y continuando con lo sugerido por las normas nacionales e internacionales y las buenas prácticas al respecto, consideramos como **resguardo** a las acciones realizadas para mantener la integridad de la prueba obtenida.

5. Propuesta de trabajo

Se sugiere realizar instrucción de trabajo para ser aplicado en el caso de los documentos o pruebas digitales de una operación, transacción obtenida por el auditor contador en su proceso de auditoría. Se expone a continuación la instrucción de trabajo correspondiente.

[5] https://www.iso.org/home.html

Tribunal de Cuentas
Mendoza

Cadena de custodia de la evidencia digital que no posee firma digital y/o electrónica

Proyecto de Instrucción de Trabajo

IT

Código: IT-ARE-ED

Revisión: 0

	Nombre del Cargo	Nombre y Apellido	Fecha
Confeccionó			
Aprobó			

1. Objetivo

Establecer una metodología a seguir para asegurar la integridad de la información que constituye la evidencia digital que, por diversas circunstancias, no posee firma digital y/o electrónica y que son respaldo de observaciones del proceso de Juicio de Cuentas.

2. Alcance

Direcciones de Cuentas y Delegación Zona Sur

3. Documentación de Referencia

Según digesto actualizado

4. Definiciones

Cadena de custodia: Es la forma metódica de obtención, recopilación y resguardo de la evidencia digital que no posee la firma digital y/o electrónica.

Evidencias digitales: es todo registro informático que sea válido y suficiente que respalda una observación de la rendición de cuenta.

Hash: se refiere a una función o método para generar claves o llaves que representen de manera unívoca a un documento, registro, archivo, etc.

Blockchain: conjunto de tecnologías para permitir llevar un registro seguro, descentralizado, sincronizado y distribuido de las operaciones digitales, sin la intermediación de terceros. Pueden ser consideradas evidencias digitales del proceso de auditoría.

5. Responsabilidades

5.1. Profesional auditor: Identificación y obtención de evidencia digital.

5.2 Responsable informático de cada área: realizar hash de las evidencias digitales, registrando el hash obtenido en el check list, consignando archivo hasheado, fecha y expediente.

6. Precauciones

6.1 En lo posible, tomar la evidencia en un formato que no altere su contenido, registrando cada uno de los pasos seguidos en este proceso.

6.2 Tener en cuenta los recaudos de las normas para la adquisición y custodia de evidencia digital.

6.3 Verificar que la evidencia no se encuentre contenida en SIGESCO o expediente electrónico firmados digitalmente. Tener en cuenta que el presente trabajo no comprende evidencia firmada digitalmente

6.4 De ser necesario, contar con los medios tecnológicos necesarios para hacer la extracción de la evidencia de manera segura (notebook, pen drive, etc.)

7. Desarrollo

Procesos que deben seguirse para la custodia de la evidencia digital: 1) obtención; 2) resguardo.

7.1) Obtención de la evidencia: Momento en el que el auditor identifica y recopila la evidencia digital, para poder tomarlo como prueba de su informe de auditoría y el cual es input del Fallo del Tribunal de Cuentas. Son ejemplos: Los archivos digitales que forman parte del juicio de cuenta, archivos primarios de recaudación, los archivos digitales que se encuentren contenidos en la plataforma digital SIGESCO remitido por el cuentadante sin firma digital; los archivos o documentos entregado en la oficina virtual (Acuerdo N°6569) sin la firma digital correspondiente; documentación contenida en expedientes digitales, y necesarios para la rendición de cuentas sin los recaudos establecidos por Ley 9003 y/o Acuerdo N°6569 HTC, o cualquier documento que se presente en el Tribunal como medio de prueba o fuere solicitado y tomado por el auditor contador mediante procedimientos de auditoría, y que no cuenten con firma digital.

7.1.1) Identificar evidencia digital a recopilar: El profesional responsable de la auditoría deberá identificar claramente los registros que requiere.

7.1.2) Al momento de recopilar la evidencia digital, si ésta no se encuentra en rendiciones de cuentas o documentación remitida al Tribunal, el profesional debería buscar la misma en la sede donde se encuentra. En este caso se debería realizar un Acta de constatación que asegure la obtención de la evidencia, y en presencia de algún responsable de la institución controlada.

7.1.3) Anotar los resultados en registro Anexo I

7.2 Resguardo de la evidencia:

7.2.1) Hashear el contenido https://hash.online-convert.com/es/generador-sha256

7.2.2) Subirlo a blockchain (BFA) https://bfa.ar/sello2#/

7.2.3) Anotar el resultado en registro consignado en el Anexo II

8. Resultado exitoso de la tarea

Evidencia protegida y registro check list confeccionado guardado en Papeles de Trabajo.

9. Unidad y Frecuencia

Un registro por cada evidencia digital que sea necesaria custodiar para respaldar los informes del juicio de cuentas.

10. Registros

ANEXO I- Check List Recolección de evidencia digital

ANEXO II- Check List Protección de evidencia digital

11. Anexos

ANEXO I- Check List Recolección de evidencia digital

ANEXO II- Check List Protección de evidencia digital

ANEXO I- Check List Recolección de evidencia digital

Expediente	
Organismo	
Ejercicio	

Identificación de la prueba

Nombre o título del elemento o archivo y extensión:.....

Dispositivo del cual se extrajo (servidor de correo, celular, PC, Tablet):.....

Otras identificaciones (Según el caso. Procedimiento seguido para su obtención): ……..

Fecha de recolección: ……..

Profesional que realiza el procedimiento:.....

Funcionario o responsable presente en la recolección, en el caso de que se encuentre la misma fuera del ámbito del Tribunal: ……

ANEXO II. Check List Protección de evidencia digital

Expediente	
Organismo	
Ejercicio	

Nombre archivo	**Ubicación**	**Hash**

6. Conclusiones y recomendaciones

La aplicación de instrucciones de trabajo para el resguardo de la documentación digital, a la labor de las distintas áreas del Tribunal implica mejorar los mecanismos de control.

La sugerencia realizada por este equipo es, como todo lo que se expone en materia de TICs (Tecnologías de la Información y Comunicación), de carácter transitorio hasta tanto salgan nuevas y mejores formas de trabajo. Tenemos muchas herramientas para abordar la temática y nos queda mucho por resolver.

Consideramos que el nuevo desafío de los órganos de control es: estudiar, analizar, planificar y ejecutar con herramientas legales, informáticas y de gestión humana, para lograr que las evidencias de auditoría digitales cumplan con el requisito de validez.

Es nuestro compromiso pensar nuevas formas de trabajo que satisfagan la misión de nuestra institución. Acuerdo 3220 (T.O. Acdo. N.° 6506) HTC *"Artículo 1º - Aprobar la "Visión" del Tribunal de Cuentas de la Provincia de Mendoza, adoptada por unanimidad de sus miembros: "SATISFACER LA NECESIDAD DE LA COMUNIDAD EN MATERIA DE CONTROL DE LA ACTIVIDAD FINANCIERO–PATRIMONIAL DEL ESTADO PROVINCIAL Y MUNICIPAL, PARA ASEGURAR SU TRANSPARENCIA Y PREVENIR ACTOS DE CORRUPCIÓN.""*

BIBLIOGRAFÍA

- Acuerdo H.T.C. N.º 3220 Tribunal de Cuentas de la Provincia de Mendoza. Texto Ordenado aprobado según Acuerdo N.º 6506 emitido el 30/10/2019
- Acuerdo 6569 Honorable Tribunal de Cuentas de Mendoza Sistemas de Gestión documental, 15 de diciembre de 2021.
- Asamblea General de las Naciones Unidas. Septuagésimo cuarto período de sesiones. Tema 109; Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos A/74/130 de fecha 30 de julio de 2019. https://www.unodc.org/documents/Cybercrime/SG_report/V1908185_S.pdf. Extraído el 9 de agosto de 2022.
- Convenio de Budapest. Extraído el 8 de agosto de 2022 de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
- Decreto N.º 1131/2016, Archivo y digitalización de expedientes, Ministerio de Modernización, 28 de octubre de 2016.
- Firma Digital. Ley N.º 25506 Congreso de la Nación Argentina. Sancionada el 14 de noviembre de 2001. Boletín Oficial 14 de diciembre de 2001.
- Guía de obtención, preservación y tratamiento de evidencia digital. Resolución 756/16 de fecha 31 de marzo de 2016. Procuración General de la Nación. Extraída de: https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf
- Glosario de Términos de Ciberseguridad; http://servicios.infoleg.gob.ar/infolegInternet/anexos/325000-329999/328599/res1523-2.pdf
- Ley de procedimiento administrativo, Ley Provincial N.º 9003, publicada en boletín oficial el 19 de septiembre de 2017.
- Norma ISO/IEC 27037 Directrices para identificación, recopilación, adquisición y preservación de evidencia digital (ciberseguridad.com)
- Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Procesos de recolección de pruebas en ciberdelitos. Resolución 234/2016 Ministerio de Seguridad de 7 de junio de 2016.