GPF-OCEX 1503: La evidencia electrónica de auditoría

Referencia: ISSAI-ES 100, NIA-ES-SP 1500 y
Manual de procedimientos de fiscalización de regularidad del Tribunal de Cuentas

Documento elaborado por la Comisión Técnica de los OCEX y
aprobado por la Conferencia de Presidentes de la ASOCEX el 20/05/2020

1. Introducción

Esta Guía práctica de fiscalización complementa la *NIA-ES-SP 1500 Evidencia de auditoría*, que es aplicable en su integridad, y proporciona orientaciones adicionales a los auditores de los OCEX en relación con la evidencia electrónica de auditoría.

Dicha norma establece que el objetivo del auditor es diseñar y aplicar procedimientos de auditoría de forma que le permita obtener evidencia de auditoría suficiente y adecuada para poder alcanzar conclusiones razonables en las que basar su opinión.

Toda evidencia de auditoría debe reunir esas dos características tanto si se trata de algún tipo de evidencia analógica tradicional como si se trata de evidencia electrónica, que en los actuales entornos de administración electrónica es la modalidad preponderante.

2. Definiciones

A los efectos de las Guías Prácticas de Fiscalización de los OCEX, los siguientes términos tienen el significado que se les atribuye a continuación:

Documento electrónico

> Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado. *(ENI[1])*

Evidencia electrónica de auditoría

> Incluirá cualquier tipo de elemento, dato, información o fichero susceptible de ser originado, tratado, transmitido y almacenado entre sistemas o aplicaciones informáticas, que haya sido

1 Esquema Nacional de Interoperabilidad (Real Decreto Real Decreto 4/2010).

utilizado para alcanzar las conclusiones que sustentan el informe de fiscalización. Por ejemplo: hoja de cálculo utilizada para calcular una estimación contable, las facturas electrónicas, los ficheros de nómina, la base de datos contable, etc.

También comprende los elementos lógicos, programas y aplicaciones utilizados en los procedimientos de gestión del fiscalizado que sean significativos por la auditoría.

Firma electrónica:

Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante. *(ENI)*

Formato

Conjunto de reglas (algoritmo) que define la manera correcta de intercambiar o almacenar datos en memoria. *(ENI)*

Marca de tiempo

La asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico. *(ENI)*

Metadato

Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación. *(ENI)*

Metadato de gestión de documentos

Información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan. *(ENI)*

Modelo de datos

Conjunto de definiciones (modelo conceptual), interrelaciones (modelo lógico) y reglas y convenciones (modelo físico) que permiten describir los datos para su intercambio. *(ENI)*

Pista de auditoría

Es la evidencia que demuestra cómo una transacción específica ha sido iniciada, procesada y registrada en el sistema de información contable. *Por ejemplo, la pista de auditoría de una compra puede incluir el pedido, el albarán de recepción, la factura, el apunte en el registro de facturas y el asiento contable.*

Registros contables

Registros de asientos contables iniciales y documentación de soporte, tales como cheques y registros de transferencias electrónicas de fondos; facturas; contratos; libros principales y libros auxiliares; asientos en el libro diario y otros ajustes de los estados financieros que no se reflejen en asientos en el libro diario; y registros tales como hojas de trabajo y hojas de cálculo utilizadas para la imputación de costes, cálculos, conciliaciones e información a revelar.

Sello de tiempo

La asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la

marca de tiempo del documento. *(ENI)*

Sellado de tiempo

Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos. *(ENI)*

3. Tipos de evidencia de auditoría

A los tradicionales tipos de evidencia de auditoría debe añadirse actualmente la evidencia electrónica, y tienen estas características distintivas[2]:

Procedimientos de auditoría para obtener evidencia	Consideraciones
FÍSICA o MATERIAL	
Inspección u observación directa de personas, propiedades o acontecimientos. Deberán documentarse en forma de memorándums, fotografías, gráficos, mapas o muestras reales.	Aunque suelen ser las pruebas más convincentes, el auditor debe tener en cuenta que, en algunos casos, su presencia puede distorsionar la realidad.
DOCUMENTAL	
Revisión de documentos y registros contables, manuales, manifestaciones de la dirección. Pueden ser tanto informaciones producidas y mantenidas por terceros o por el ente auditado.	La información útil puede no estar siempre documentada, lo que exige también la aplicación de otros enfoques.
ORAL o TESTIMONIAL	
Indagación o entrevistas al personal de la entidad o a terceras partes, documentadas o corroboradas siempre que sea posible. Estas evidencias deben ser corroboradas por otras evidencias y ser evaluadas atendiendo su origen.	Salvo en casos excepcionales, el auditor no aceptará como fiable por sí sola la información obtenida en entrevistas. (La fiabilidad de la evidencia de auditoría es mayor si es obtenida directamente por el auditor que si lo es indirectamente o si se obtiene por inferencia y en forma documental que solo oralmente)
ANALÍTICA	
Análisis mediante razonamiento, reclasificación, cálculo y comparación.	Esta evidencia se obtiene ejerciendo el juicio profesional para evaluar la evidencia física, documental y oral.
ELECTRÓNICA	
Para su obtención puede ser necesario utilizar herramientas informáticas de auditoría.	Para validar su fiabilidad normalmente será necesario revisar los controles internos (CGTI). En entornos complejos será indispensable la colaboración de especialistas en auditoría informática.

2 Fuente: Manual de auditoría financiera y de cumplimiento del Tribunal de Cuentas Europeo, edición 2012, página 52.

4. Consideraciones generales sobre la evidencia electrónica de auditoría

La implantación de sistemas de información automatizados en la administración ha provocado que la pista visible de muchas transacciones que rastreamos los auditores en las fiscalizaciones haya desaparecido físicamente, transformándose en algo más intangible.

En muchas entidades, los registros de las operaciones y del resto de la información capturada estarán soportados electrónicamente, constituyendo el soporte único y suficiente que garantice su conservación. Las bases de datos del sistema informático donde residan los registros contables constituirán soporte suficiente para la llevanza de la contabilidad de la entidad contable, sin que sea obligatoria la obtención y conservación de libros de contabilidad.[3]

La justificación de los distintos hechos contables estará soportada en documentos electrónicos. No vamos a disponer de documentos físicos para revisarlos, comprobar firmas, fotocopiar, poner tildes, etc[4]. Las facturas de proveedores llegan en formato electrónico desde el exterior a través de FACe, y solo existen en formato electrónico. Los datos pueden consistir en simples registros de una base de datos o documentos electrónicos complejos (factura electrónica, documentos pdf, correos electrónicos, etc).

Los siguientes aspectos resultan de particular relevancia para el auditor, cuando la evidencia de auditoria se encuentra disponible en formato electrónico:

- El riesgo de que la información que soporta los saldos y transacciones reflejados en los registros contables sea destruida o alterada y dicha destrucción o alteración no sea detectada se incrementa cuando dicha información se inicia, autoriza, procesa y almacena únicamente en formato electrónico y no existen controles adecuados y efectivos al respecto.

  En estas circunstancias, el auditor debe considerar si el diseño, implementación y operatividad de los controles existentes sobre la seguridad de la información son adecuados para prevenir cambios no autorizados a los sistemas y registros contables, o a los sistemas que proporcionan datos relevantes relacionados con la información financiera objeto de su revisión.

  Por ejemplo, al considerar la integridad de la evidencia en formato electrónico el auditor puede realizar pruebas de cumplimiento sobre controles automáticos tales como pruebas de integridad de registro, firmas electrónicas y control de versiones. Dependiendo de la evaluación de estos controles, el auditor puede considerar la realización de procedimientos de auditoría adicionales.

---

3 Véase por ejemplo la Orden HAP/1781/2013, de 20 de septiembre, por la que se aprueba la Instrucción del modelo normal de contabilidad local, cuya Regla 15 establece que

> "2. Las **bases de datos** del sistema informático donde residan los registros contables constituirán soporte suficiente para la llevanza de la contabilidad de la entidad contable, sin que sea obligatoria la obtención y conservación de libros de contabilidad en papel o por medios electrónicos, informáticos o telemáticos."

4 Por ejemplo, la misma Instrucción establece:

> "Regla 37. Autorización.
>
> 2. Cuando las operaciones se incorporen al sistema mediante la utilización de soportes electrónicos, informáticos o telemáticos, los procedimientos de autorización y control mediante diligencias, firmas manuscritas, sellos u otros medios manuales podrán ser sustituidos por **autorizaciones y controles** establecidos en las propias aplicaciones informáticas que garanticen la identificación y el ejercicio de la competencia por quien la tenga atribuida.
>
> Regla 38. Toma de razón.
>
> 2. En el caso de que las operaciones sean registradas a partir de los datos contenidos en soportes electrónicos, informáticos o telemáticos, la diligencia de toma de razón se sustituirá por los oportunos **procesos de validación en el sistema**, mediante los cuales dichas operaciones queden referenciadas en relación con las anotaciones contables que hayan producido."

- En ocasiones (por ejemplo, en el caso de entidades que utilicen sistemas de "administración electrónica" o de "procesamiento de imágenes" para el escaneado de documentos y su posterior almacenamiento y consulta), los documentos originales, tales como órdenes de compra, albaranes de entrega, facturas y similares, pueden existir únicamente en formato electrónico o haberse eliminado una vez han sido escaneados. En estas circunstancias, la suficiencia y adecuación de la evidencia de auditoría generalmente dependerá de la efectividad de los controles internos existentes para asegurar la exactitud e integridad del registro electrónico de la información.
- La naturaleza y momento de ejecución de los procedimientos de auditoría a realizar pueden verse afectados por el hecho de que parte de los datos contables y otra información puede existir o estar disponible únicamente en momentos concretos o por periodos de tiempo limitado. En ocasiones, dicha información ya no puede obtenerse con posterioridad si los archivos electrónicos a partir de los cuales se ha generado han sufrido cambios y no existen copias de seguridad de los mismos. En estas circunstancias, será necesario que el auditor ejecute sus procedimientos en el momento en que la información está disponible o bien que solicite la retención específica de la información necesaria para la ejecución de sus procedimientos de auditoría.

5. Características de la evidencia electrónica de auditoría

La obtención de evidencia electrónica o informática suficiente y adecuada se realiza a través de la información y datos contenidos en ficheros o soportes electrónicos, informáticos, telemáticos o en las bases de datos procedentes de aplicaciones y sistemas. Por tanto, incluirá cualquier tipo de elemento, dato o fichero susceptible de ser originado, tratado, transmitido y almacenado entre sistemas o aplicaciones informáticas.

La evidencia informática se caracteriza por la **dificultad de su obtención y tratamiento a través de los métodos tradicionales** de auditoría y, si bien es cierto que los objetivos específicos de la fiscalización no se ven afectados por el hecho de que los datos financieros y contables se procesen manualmente o mediante sistemas y aplicaciones informáticas, **los métodos para obtener la evidencia de auditoría sí se ven manifiestamente influenciados por estos procesos.** En el Anexo se aporta información adicional sobre las características de la evidencia electrónica de auditoría.

A fin de poder valorar la suficiencia y lo apropiado de la evidencia informática recopilada para respaldar el informe de auditoría, el auditor debe considerar los riesgos específicos asociados al uso de este tipo de evidencia. Estos riesgos no pueden ser evaluados únicamente revisando la evidencia documental, como suele hacerse con los documentos en papel.

La copia impresa de información en soporte digital o la lectura de la información directamente de la pantalla del ordenador es solamente un formato. Y éste no proporciona ninguna indicación del origen y autorización, ni tampoco garantiza la integridad ni la compleción de la información. Los auditores deberían asegurar que los controles y las distintas tecnologías utilizadas para crear, procesar, transmitir y guardar información en soporte informático son suficientes para garantizar su fiabilidad.

Por ejemplo, cuando se haga una prueba sobre facturas recibidas con el sistema FACe, hay que tener muy claro que las copias en papel de facturas no son realmente copias, sino visualizaciones completas o incompletas de los ficheros informáticos y que esas visualizaciones son una evidencia muy débil. La evidencia válida está en los ficheros informáticos, a los que debemos acceder.

6. Diligencia y escepticismo profesionales

El escepticismo profesional es una actitud que requiere mentalidad o espíritu crítico y una evaluación crítica de la evidencia de auditoría. Significa no confiar únicamente en las manifestaciones del auditado y no dar por sentado, sin otra evidencia corroborativa, que los registros proporcionados por el auditado son auténticos.

Esto puede plantear problemas a veces, cuando los registros informáticos (evidencia electrónica de transacciones o saldos) sólo pueden ser corroborados por otra evidencia informática. En estos casos su autenticidad y fiabilidad puede ser difícil o imposible de verificar sin conocer los controles automatizados o informáticos relacionados y hacer pruebas sobre su eficacia operativa (pruebas de controles).

Se utilizan muchos documentos o listados en papel, generados informáticamente (el pdf de una factura electrónica o un listado de nómina, por ejemplo), o guardados en formato digital. Estos listados y documentos, sobre los que se realizan determinadas comprobaciones, son tan sólo una **visualización "física" de una evidencia electrónica,** que podrían haber sido fácilmente alterados para engañar al auditor. Sin embargo, en muchas ocasiones las pruebas que se realizan sobre dichos documentos son casi las mismas que hace 40 años, raras veces se comprueban los controles de seguridad e integridad (por ejemplo) utilizados en la generación de esos listados y en las bases de datos fuentes de estos, dando implícitamente por supuesto que existen. Cuando se actúa así, se está incurriendo en un riesgo importante de auditoría y se resiente la diligencia profesional exigida.

Las Normas de Auditoría del Sector Público (5.3.10) de la IGAE recogía esta idea: ***"Cuando se emplee evidencia informática, o datos procedentes de sistemas informáticos del auditado, los auditores deberán evaluar la fiabilidad de esta evidencia, y no darla nunca por supuesta a priori."***

Cuanto más complejo sea el *entorno informático* mayor será el grado de escepticismo profesional requerido para evaluar la evidencia electrónica.

7. Fiabilidad de la evidencia electrónica

La fiabilidad de la información que se utilizará como evidencia depende de su origen (fuente) y su naturaleza, así como de las circunstancias específicas en las que se obtuvo, incluido, cuando sean relevantes, los controles sobre su preparación y conservación. **Esto es especialmente importante cuando se trata de información y datos en formato electrónico**.

La obtención de evidencia informática se distingue de la tradicional (identificación de las fuentes de información disponibles, recogida, análisis de evidencia y confirmación de la misma), por lo siguiente:

- Tener una pluralidad de formatos.
- La dificultad de establecer su origen.
- La facilidad de alteración o duplicación.
- Las dificultades para comprobar la forma de su aprobación y firma.

Es por ello por lo que **el equipo auditor, al emplear la evidencia informática, deberá garantizar la fiabilidad de la misma además de asegurar que las tecnologías y aplicaciones empleadas para generar, transmitir, editar y almacenar la información son también confiables.**

Cuando se utilicen técnicas y herramientas informáticas de análisis de volúmenes masivos de datos deberá considerarse cuidadosamente qué controles debe revisar el auditor para validar las bases de datos de donde se ha extraído la información.

El auditor deberá actuar con diligencia y escepticismo profesional y hacerse preguntas como las siguientes para asegurarse de la fiabilidad y exactitud de la información:

¿Qué datos son usados para elaborar el informe recibido?

¿Qué aplicación ha procesado los datos?

¿Los datos o informe que nos han proporcionado pueden ser susceptibles de cambios manuales?

¿Cuál es la probabilidad de que este listado u otro documento informático sean incorrectos, ya sea accidental o intencionadamente?

¿Quiénes, de la organización auditada, tienen la oportunidad y la motivación para alterar los datos electrónicos?

¿Puede alterarse la evidencia informática sin dejar pistas de auditoría o rastros del cambio?

¿Hay una pista de auditoría que liga claramente la evidencia informática al hecho que la generó y a su inclusión en las cuentas anuales?

¿Contiene la evidencia informática información que identifique quién la generó y cuándo?

¿Qué controles existen para prevenir cambios no autorizados en la evidencia informática después de su correcta generación?

¿Quién tiene derechos de acceso para cambiar la evidencia informática?

¿Cómo sabe el auditor que la evidencia informática no ha sido intencionadamente alterada para engañar o llevar a conclusiones equivocadas?

¿Tienen el sistema un "log" de auditoría adecuadamente establecido para registrar los intentos de acceso (éxitos y fracasos) a la evidencia informática?

¿Han sido revisados los "log" de auditoría por alguien independiente?

¿Son efectivos los CGTI de la aplicación que ha procesado los datos y generado el informe?

¿Hemos verificado específicamente algún control sobre la completitud y exactitud de los datos utilizados? ¿Son efectivos?

La respuesta a estas cuestiones ayudará al auditor a evaluar la fiabilidad de los datos informáticos que se utilizan como evidencia y el riesgo de que existan incorrecciones significativas, y a planificar pruebas de auditoría más eficaces, incluyendo la necesidad de que participe un experto en auditoría informática.

La evaluación de la exactitud y la integridad, y si es adecuada como evidencia, debe efectuarse tanto para la evidencia tradicional como para la obtenida mediante herramientas y técnicas de análisis de datos. Pero al utilizar herramientas de este tipo, se obtiene la información directamente de los ficheros maestros y de transacciones contenidos en las bases de datos subyacentes en los sistemas de información.

Dicho todo lo anterior, debe tenerse claro que un auditor no tiene que ser un especialista en la obtención y examen de la evidencia informática para darse cuenta de que la información proporcionada por los ordenadores no es fiable si no hay otra evidencia corroborativa, o si no se ha realizado y documentado una revisión de los controles generales y de aplicación.

Los **criterios o propiedades** que permitirán valorar la fiabilidad de la información y garantizar la misma como evidencia de fiscalización en los entornos informatizados son coincidentes con las cinco dimensiones de la seguridad de la información que establece el Esquema Nacional de Seguridad:

- **Confidencialidad**, es la propiedad de la información por la que se garantiza que está accesible

únicamente a personal autorizado a acceder a dicha información.

- **Integridad**, es la propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.
- **Disponibilidad**, se trata de la capacidad de un servicio, un sistema o una información, de ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.
- **Autenticidad**, es la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **Trazabilidad**, es la propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

El cumplimiento de estas propiedades se debe revisar examinando los CGTI.

Además, se deben asegurar la completitud y la exactitud, mediante la revisión de controles de aplicación y la realización de procedimientos sustantivos.

8. Suficiencia de la evidencia

Cuando se trabaja con evidencia electrónica es una cuestión de juicio profesional determinar cuándo se considera que se ha obtenido suficiente evidencia.

La generalización de la administración electrónica viene acompañada por una realidad inevitable: toda la información de gestión útil para las fiscalizaciones está en alguna tabla de alguna base de datos. La utilización de ERP y el Big Data ha hecho que proliferaran las grandes bases de datos como fuente de evidencia.

La auditoría con metodología actualizada permite que el auditor sepa cuáles son las tablas y las bases de datos con la información necesaria y pueda obtenerla. Una vez disponibles los ficheros fuente, mediante la utilización de técnicas/herramientas de análisis de datos, el auditor puede realizar muchas pruebas sobre el 100% de la población, no solo sobre muestras. Esta circunstancia permite maximizar la percepción de la suficiencia de la evidencia.

9. Procedimientos de auditoría aplicables

Los objetivos específicos de auditoría no se ven afectados por el hecho de que los datos contables se procesen manualmente o mediante ordenador. Sin embargo, los métodos para obtener la evidencia de auditoría adecuada y suficiente pueden verse influenciados por los procesos informáticos. El auditor puede utilizar tanto procedimientos manuales como técnicas de auditoría asistidas por ordenador, o bien una combinación de ambos métodos, al objeto de obtener dicha evidencia electrónica. Sin embargo, en algunos sistemas contables complejos que utilizan un ordenador para llevar a cabo aplicaciones significativas, puede ser difícil o imposible que el auditor obtenga ciertos datos sin apoyo de especialistas.

La obtención y el análisis de evidencia electrónica debe analizarse desde una doble perspectiva:

a) Revisando la información y bases de datos disponibles mediante pruebas realizadas con herramientas informáticas de auditoría.

Se hace necesario desarrollar nueva metodología de auditoría e introducir nuevas técnicas y herramientas informáticas para poder obtener, manejar y evaluar este tipo de evidencia electrónica. Será el momento de utilizar herramientas y técnicas de análisis de datos. Con este

tipo de evidencia debe seguirse la *GPF-OCEX 5370 Guía para la realización de pruebas de datos*.

b) Evaluando el entorno de los sistemas de información del ente fiscalizado, efectuando pruebas de los controles internos implantados en los programas y aplicaciones informáticas.

La revisión de los procedimientos administrativos y contables, el flujo de documentos, autorizaciones, segregación de funciones, etc. existentes en el seno de la organización auditada ha formado parte siempre de los procedimientos ordinarios de auditoría. En este sentido, la revisión de los sistemas informáticos de gestión proporciona evidencia de auditoría, indispensable, ya que nos permite conocer cuál es el flujo de las transacciones, de los documentos electrónicos, las autorizaciones explícitas e implícitas, la segregación de funciones realmente existente, los controles de seguridad implementados frente a accesos y modificaciones no autorizados, y otros procedimientos de control interno.

Actualmente, con sistemas complejos que interrelacionan e integran distintas áreas funcionales de las organizaciones, y la desaparición progresiva del soporte papel, el análisis y evaluación de tales sistemas **excederá normalmente las competencias de un auditor financiero, requiriéndose la intervención de un especialista en auditoría informática**.

Para revisar el sistema de control interno pueden utilizarse las guías *GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información (CGTI) en un entorno de administración electrónica* y *GPF-OCEX 5340 Los controles de aplicación: qué son y cómo revisarlos.*

De acuerdo con la NIA-ES-SP 315 / GPF-OCEX 1315 el auditor debe tener en cuenta el entorno informatizado en el diseño de los procedimientos de auditoría necesarios para reducir el riesgo de auditoría a un nivel aceptable Estas normas exigen al auditor la revisión de los sistemas de control automatizados, la valoración del riesgo de auditoría correspondiente y la realización de pruebas de controles.

Aunque se deberán efectuar en todo caso pruebas sustantivas manuales para verificar transacciones y saldos de importe significativo, es muy importante tener en cuenta que, **en determinadas situaciones, no será posible reducir el riesgo de detección a un nivel aceptable realizando únicamente pruebas sustantivas manuales, siendo preciso combinarlas con pruebas de controles.**

10. Colaboración de especialistas

Tanto la obtención de evidencia electrónica de los sistemas de información del auditado como su análisis, ya se trate de ficheros, como de la revisión de controles internos automatizados implantados en los sistemas, requerirá capacidades profesionales, técnicas y procedimientos de auditoría específicos. Cuanto mayor sea la complejidad del sistema de información del ente auditado más necesaria será que los equipos de auditoría cuenten con la colaboración de **auditores de sistemas de información** y de **expertos** en el uso de herramientas y técnicas de análisis de datos.

Anexo Consideraciones adicionales sobre la evidencia electrónica de auditoría

1. Los documentos electrónicos en la Ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

La Ley 39/2015 aborda aspectos esenciales para garantizar la autenticidad de los documentos electrónicos, su autoría y/o aprobación, y dedica parte de su articulado a una de las novedades más importantes de la Ley: la separación entre identificación y firma electrónica y la simplificación de los medios para acreditar una u otra, de modo que, con carácter general, sólo será necesaria la primera, y se exigirá la segunda cuando deba acreditarse la voluntad y consentimiento del interesado.

Se establece, con carácter básico, un conjunto mínimo de categorías de medios de identificación y firma a utilizar por todas las Administraciones. Se admitirán como **sistemas de identificación** cualquiera de los sistemas de firma admitidos, así como sistemas de clave concertada y cualquier otro que establezcan las Administraciones Públicas[5].Se admitirán como **sistemas de firma**[6]:

- los sistemas de firma electrónica cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica, expedidos por prestadores incluidos en la lista de confianza;
- los sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados cualificados de sello electrónico expedidos por prestadores incluidos en la lista de confianza;
- cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan.

La Ley 39/2015 establece que los documentos administrativos serán **digitales por defecto**. El artículo 26.1 señala que "*Se entiende por documentos públicos administrativos los válidamente emitidos por los órganos de las Administraciones Públicas.* ***Las Administraciones Públicas emitirán los documentos administrativos por escrito, a través de medios electrónicos****, a menos que su naturaleza exija otra forma más adecuada de expresión y constancia".* Continúa el apartado dos del mismo artículo diciendo que *"Para ser considerados* ***válidos****, los* ***documentos electrónicos*** *administrativos deberán:*

a) Contener ***información*** *de cualquier naturaleza archivada en un soporte electrónico según un formato determinado susceptible de identificación y tratamiento diferenciado.*
b) Disponer de los ***datos de identificación*** *que permitan su individualización, sin perjuicio de su posible incorporación a un expediente electrónico.*
c) Incorporar una ***referencia temporal*** *del momento en que han sido emitidos.*
d) Incorporar los ***metadatos*** *mínimos exigidos.*
e) Incorporar las ***firmas electrónicas*** *que correspondan de acuerdo con lo previsto en la normativa aplicable.*

Se considerarán válidos los documentos electrónicos que cumpliendo estos requisitos, sean trasladados a un tercero a través de medios electrónicos."

Respecto de su **conservación**, los artículos 17 de la Ley 39/2015 y 46 de la Ley 40/2015 establecen que los documentos administrativos se almacenarán por medios electrónicos y deberán conservarse en un formato que permita garantizar su:

- autenticidad
- integridad
- conservación

5 *Artículo 9.* ***Sistemas de identificación*** *de los interesados en el procedimiento.*

6 *Artículo 10.* ***Sistemas de firma*** *admitidos por las Administraciones Públicas.*

- disponibilidad y accesibilidad

Los medios o soportes en que se almacenen documentos deberán contar con medidas de seguridad, de acuerdo con lo previsto en el **Esquema Nacional de Seguridad**, que garanticen su:

- autenticidad
- integridad
- confidencialidad
- calidad
- protección y conservación
- la identificación de los usuarios y el control de accesos
- el cumplimiento de las garantías previstas en la legislación de protección de datos.

2. Características de la evidencia electrónica de auditoría vs la evidencia tradicional

De acuerdo con el apartado 5.3.2 de las NASP, la evidencia electrónica o informática queda definida como:

"Información y datos contenidos en soportes electrónicos, informáticos y telemáticos, así como los elementos lógicos, programas y aplicaciones utilizados en los procedimientos de gestión del auditado. Esta evidencia informática incluirá los elementos identificados y estructurados que contienen texto, gráficos, sonidos, imágenes o cualquier otra clase de información que pueda ser almacenada, editada, extraída e intercambiada entre sistemas de tratamiento de la información, o usuarios de tales sistemas, como unidades diferenciadas."

Un primer análisis de esta definición pone de manifiesto la distinción entre dos tipos de evidencia, por un lado información y datos y por otros programas y aplicaciones, de características muy diferenciadas y **que requerirán capacidades profesionales, técnicas y procedimientos de auditoría específicos**.

Hay que tener presente que los atributos de la evidencia electrónica son diferentes de los de la evidencia tradicional en varios aspectos. En el siguiente cuadro se señalan las principales diferencias.[7]

Evidencia de auditoría tradicional	Evidencia informática de auditoría
Origen	
Se puede establecer con facilidad el origen/procedencia.	Es difícil determinar el origen si únicamente se examina información en soporte informático. Se requiere la utilización de controles y de técnicas de seguridad que permitan la autenticación y reconocimiento.
Alteración	
La evidencia en papel es difícil de alterar sin que se detecte.	Es difícil, si no imposible, detectar cualquier alteración únicamente mediante el examen de la información en soporte informático. La integridad de la información depende de los controles fiables y de las técnicas de seguridad empleadas.
Aprobación	
Los documentos en papel muestran la prueba de su aprobación en su superficie.	Es difícil de establecer la aprobación si únicamente se examina la información en soporte informático. Se requiere la utilización de controles y de técnicas de seguridad.
Completitud	
Todos los términos relevantes de una transacción se incluyen por lo general en un mismo documento.	Los términos más significativos aparecen a menudo en distintos archivos de datos.

7 Véase: Émond, Caroline; Electronic Audit Evidence; The Canadian Institute of Chartered Accountants, 2003.

Evidencia de auditoría tradicional	Evidencia informática de auditoría
Lectura	
No se requiere ningún tipo de herramienta o equipo.	Es necesaria la utilización de distintas tecnologías y herramientas.
Formato	
Parte integral del documento.	El formato viene separado de los datos y puede modificarse.
Disponibilidad y accesibilidad	
Normalmente no es una restricción durante la fiscalización.	Las pistas de auditoría puede que no estén disponibles en el momento de la auditoría y el acceso a los datos puede resultar más difícil.
Firma	
Es sencillo firmar un documento en papel y comprobar la firma.	Se necesitan las tecnologías adecuadas para realizar una firma electrónica fiable y revisarla.

3. Documentación de la evidencia electrónica de auditoría

3.1 Correos electrónicos

Los auditores conservarán en el expediente de auditoría (papeles de trabajo) las comunicaciones por correo electrónico importantes, enviadas o recibidas de un organismo oficial o de un tercero, que sean relevantes para la auditoría y estén relacionadas con el informe.

El requisito de conservar las comunicaciones por correo electrónico de la entidad depende de la importancia de la correspondencia y de si la correspondencia representa evidencia de auditoría (pruebas, observaciones, u otros hallazgos).

Las comunicaciones por correo electrónico entre los miembros del equipo de auditoría se conservarán en el expediente de auditoría si se refieren a un asunto importante y contienen información o datos relevantes.

Los auditores copiarán todos los correos electrónicos importantes desde sus buzones de correo electrónico personal al expediente de auditoría antes de que finalice el trabajo, y eliminarán cualquier copia de los correos electrónicos de sus buzones cuando la documentación del expediente esté completa.

Los auditores copiarán la documentación de auditoría almacenada temporalmente en llaves USB u otros medios de almacenamiento al expediente de auditoría, y borrarán los documentos de la ubicación temporal tan pronto como sea posible y antes de que la documentación del expediente esté completa.

Todo el material, con independencia del formato o ubicación, que no se haya integrado en los papeles de trabajo y que ya no se necesite se eliminará antes de finalizar la compilación final del expediente.

El objetivo general es que el expediente de auditoría sea el único depositario de toda la documentación que sea necesario conservar en relación con la auditoría.

Los mensajes de correo electrónico han de mantener su estructura, contenido y su contexto. La estructura se refiere a la presentación del mensaje y los documentos adjuntos y mensajes relacionados. El contexto se refiere a la información que documenta el origen y el destino del mensaje, el asunto, fechas, y otra información pertinente.

A fin de conservar su valor como evidencia, los mensajes de correo electrónico deberán conservarse de un modo que no puedan ser alterados o manipulados.

3.3 Tratamiento de textos, hoja de cálculo, presentación, o documentos análogos

El tratamiento de textos, las hojas de cálculo, la presentación o los documentos análogos también forman parte de la documentación de auditoría y son almacenados temporalmente en llaves USB, en discos duros locales, servidores centrales u otros medios de almacenamiento.

Los miembros del equipo deben transferir cualquiera de estos documentos temporalmente almacenados fuera del expediente (papeles de trabajo) al interior de este antes de su finalización. Se debe tener en cuenta que tales documentos pueden haber sido ya guardados como adjuntos a correos electrónicos o como otros papeles de trabajo. En este caso, no es necesario guardar las copias adicionales del mismo documento. Una vez las envían, los miembros del equipo pueden **eliminar estos documentos de la ubicación original**. Cualquier otra información que no sea transferida al expediente es considerada similar a un archivo de escritorio y es eliminada.

En todo caso se deberán adoptar medidas de seguridad para proteger la confidencialidad e integridad de los papeles de trabajo electrónico, incluyendo medidas de encriptación de datos.

3.4 Trabajo de análisis de datos realizado con herramientas informáticas de análisis de datos

El trabajo de auditoría realizado usando ACL/IDEA[8] debe ser debidamente documentado y supervisado, como cualquier otro trabajo de auditoría. No obstante, dada la naturaleza intangible de la evidencia digital debe extremarse el cuidado en la documentación y el control de calidad del trabajo realizado, con objeto de que sea comprendido posteriormente por otro auditor y, en su caso, pueda ser reutilizado.

La documentación de una prueba compleja incluirá la siguiente documentación:

- Descripción del modelo de datos o bases de datos del sistema de información.
- Resumen de las principales reuniones mantenidas.
- Escritos de solicitud de los datos necesarios o las instrucciones para su obtención.
- Scripts utilizados o historia de las tablas finales con los resultados.
- Diagramas de flujo de la prueba de ACL/IDEA.
- Hoja de Excel/Word con las conclusiones y resultados obtenidos.

Toda esta documentación se incorporará a los papeles de trabajo de la fiscalización correspondiente como evidencia para soportar las conclusiones obtenidas.

Cuanto más sencilla sea una prueba más simple podrá ser su documentación.

La forma de solicitar la información, los datos obtenidos y las pruebas realizadas se deben documentar de tal manera que cualquier persona sin conocimiento previo de la entidad y con conocimientos funcionales de ACL/IDEA, pueda comprender los objetivos de la prueba, la información de la que se ha dispuesto, su tratamiento, los resultados y el fundamento de las conclusiones a las que se ha llegado. Por esta razón es importante que los OCEX estandaricen cómo se deben realizar estas pruebas.

Se incluirá en el archivo permanente toda la información que pueda ser de utilidad para realizar las pruebas de datos en la entidad fiscalizada en ejercicios sucesivos: descripción del modelo de datos o bases de datos, modelos de solicitud de los datos, diagramas de flujo de datos de la ejecución de las pruebas, scripts de ejecución de las pruebas, etc.

Si la prueba está bien documentada (incluyendo scripts y diagramas de flujo descriptivos), en años posteriores será muy **sencillo y rápido** repetirla por otras personas distintas de las que la crearon, ejecutaron y documentaron.

Una buena documentación de la prueba de datos realizada permite:

- Verificar la calidad del diseño de la prueba y la razonabilidad de sus resultados.

8 ACL e IDEA son dos de las herramientas informáticas de auditoría más habituales en el mundo de la auditoría. No obstante, los comentarios son aplicables a cualquier otra herramienta con similares funcionalidades.

- Respaldar las conclusiones de auditoría que se hayan obtenido.
- Independizar la ejecución de la prueba de la persona que la haya diseñado.
- Disminuir significativamente el coste de ejecución en años posteriores.

Con este tipo de evidencia se seguirán las indicaciones sobre documentación indicadas en la *GPF-OCEX 5370 Guía para la realización de pruebas de datos*.

4. Ejemplos de nuevas evidencias electrónicas

4.1 La factura electrónica

Una factura electrónica es una factura que se expide y recibe en formato electrónico y tiene los mismos efectos legales que una factura en papel. Recordemos que una factura es un justificante de la entrega de bienes o la prestación de servicios.

Es obligatorio su uso, para los proveedores personas jurídicas que hayan entregado bienes o prestado servicios a cualquier administración pública, desde el 15/1/2015, en los términos establecidos en el artículo 4.de la ley 25/2013, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público.

Legibilidad, autenticidad e integridad

Todas las facturas, sean electrónicas o en papel, deben garantizar:

- La legibilidad de la factura.
- La autenticidad del origen de la factura (es decir, garantizar la identidad del obligado a su expedición y del emisor de la factura, que pueden ser la misma persona).
- La integridad del contenido de la factura (es decir, garantizar que su contenido no ha sido modificado).

En el caso de la factura electrónica, la legibilidad la facilita el programa informático que la crea o recibe.

La autenticidad y la integridad se pueden garantizar de diversas formas:

- Mediante firma electrónica avanzada basada en un certificado reconocido.
- Mediante intercambio electrónico de datos EDI.
- Mediante otros medios que los interesados hayan comunicado a la Agencia Estatal de Administración Tributaria con carácter previo a su utilización y hayan sido validados por la misma.
- Mediante los controles internos pertinentes, siempre que permitan crear una pista de auditoría fiable que establezca la necesaria conexión entre la factura y la entrega de bienes o prestación de servicios que la misma documenta.

FACe

Uno de los sistemas más utilizados en la Administración es **FACe**. Es el Punto General de Entrada de Facturas de la Administración General del Estado, creado al amparo del artículo 6 de la Ley 25/2013, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público. Está abierto a que sea usado por terceras Administraciones Públicas, y permite la remisión de facturas en formato electrónico a aquellos organismos de las administraciones que estén dados de alta en el sistema[9].

FACe proporciona a las Administraciones Públicas dos formas de acceso al servicio:

9 Actualmente lo utilizan más de 8.200 entidades de todos los ámbitos del sector público (estatal, autonómico y local).

- Portal Web de FACe: Portal a través del cual el organismo accede al buzón o buzones de sus unidades (oficina contable, órgano gestor, unidad tramitadora) y puede descargarse la factura electrónica y los anexos que ha presentado el proveedor y actualizar el estado de tramitación de la factura para que sea notificado al proveedor.
- Interfaz de servicios web: interfaz que permite que el sistema informático que da soporte al registro contable de facturas de la Administración destinataria pueda descargarse las facturas de manera automática sin la necesidad de acción humana en la descarga de la factura desde FACe.

Dentro del documento de factura electrónica (.xsig) es obligatorio, para la correcta remisión de la factura al órgano destinatario final, que el proveedor informe del órgano gestor, la unidad tramitadora y la oficina contable destinatarios, datos que le deben ser facilitados por la administración correspondiente[10].

No obstante, para facilitarle al proveedor la cumplimentación de esta información, el portal www.face.gob.es dispone de un directorio donde localizar las unidades de cada organismo y obtener el código DIR que deben indicar dentro de la factura.

Problemática planteada a los auditores

Normalmente la entidad fiscalizada adherida a FACe tendrá todas las facturas electrónicas descargadas en su sistema de información[11].

10 *¿Qué se entiende por oficina contable?*

La unidad o unidades que tienen atribuida la función de contabilidad en el organismo y que también son competentes para la gestión del registro contable de facturas.

¿Qué se entiende por órgano gestor?

Centro directivo, delegación, subdelegación territorial u organismo de la Administración General del Estado, Comunidad Autónoma o Entidad Local a que corresponda la competencia sobre la aprobación del expediente de gasto.

¿Qué se entiende por unidad tramitadora?

Órgano administrativo al que corresponda la tramitación de los expedientes, sin perjuicio de a quien competa su aprobación.

11 Si la entidad dispone de un sistema automatizado de registro contable de facturas conectado a FACe, las facturas solo podrán ser descargadas por el sistema del registro contable de facturas conectado con FACe, no permitiendo descargarlas a través del portal de gestión de facturas interno.

Sin embargo, si la entidad no dispone de dicho sistema automatizado y utiliza el portal de gestión de facturas interno, el sistema permite el acceso a los usuarios, mediante certificado electrónico, a los buzones asociados a sus unidades donde pueden consultar las facturas recibidas. El sistema permite la descarga de las facturas originales (extensión .xsig) en formato facturae 3.2/3.2.1, documentos anexos y la descarga de un resumen de la factura en formato PDF donde se incluye la factura completa

Al fiscalizar el capítulo 2 o el 6 se deberá considerar, entre otras muchas cosas, si:

- Las BD con las facturas electrónicas que hemos obtenido contienen todas las facturas enviadas por FACe.
- Las impresiones en papel o pdf que nos proporcione la entidad están incompletas o son incorrectas.
- Es más seguro, eficaz y eficiente realizar las pruebas diseñadas sobre el 100% de las facturas en formato electrónico en vez de sobre una muestra impresa en papel.
- Se deben realizar pruebas sobre la integridad de las facturas electrónicas (revisión de metadatos).
- Se ha cumplido lo dispuesto en el artículo 12 de la Ley 25/2013 respecto de la obligación de realizar auditorías de sistemas anuales.
- Etc.

3.2 El nuevo sistema de gestión del IVA basado en el Suministro Inmediato de Información (SII), una fuente de evidencia de auditoría electrónica

El Real Decreto 596/2016, de 2 de diciembre, para la modernización, mejora e impulso del uso de medios electrónicos en la gestión del Impuesto sobre el Valor Añadido, introdujo un nuevo sistema para la llevanza de los libros registro en sede electrónica, que no solo facilita la lucha contra el fraude fiscal, sino que supone una mejora en la calidad de los datos y en la correcta aplicación de las prácticas contables, así como un ahorro de costes y una mayor eficiencia que redunda en beneficio de todos los agentes económicos.

El colectivo incluido obligatoriamente en el "SII" está integrado por todos aquellos sujetos pasivos cuya obligación de autoliquidar el Impuesto sobre el Valor Añadido sea mensual, por ejemplo, las grandes empresas con facturación superior a 6 millones de euros anuales.

El contribuyente dispone en la Sede electrónica de la AEAT de un Libro Registro "declarado" y otro "contrastado" con la información de contraste procedente de terceros que pertenezcan al colectivo de este sistema o de la base de datos de la AEAT. Es decir, la información obtenida a través del SII por parte de la Agencia Tributaria será puesta a disposición de aquellos empresarios o profesionales con quienes hayan efectuado operaciones aquellas personas y entidades que, bien de forma obligatoria o tras ejercer la opción, lleven los libros registro a través de la Sede electrónica, lo que constituye una herramienta de asistencia al contribuyente que puede resultar de gran utilidad para el auditor al tener la posibilidad de disponer de una información muy valiosa para obtener evidencia de auditoría, mediante el contraste de esta información.

El auditor puede obtener evidencia electrónica sobre las facturas que aparecen registradas en la contabilidad de la empresa que está auditando, puede contrastar la información con FACe y ahora con la información que han declarado a la AEAT los emisores o receptores de las facturas a través del sistema «SII». Esta nueva forma de obtención de evidencia electrónica podría reducir, e incluso, en determinadas circunstancias, reemplazar, los tradicionales procedimientos de circularización a clientes y proveedores.

El auditor puede obtener los archivos mensuales de facturas, los cuales pueden ser capturados por el cliente, en presencia del auditor, posteriormente podrá ser conciliada la facturación declarada en el sistema «SII» con los registros contables de la empresa, también podrá comprobar si estas facturas han sido contrastadas por la contraparte, lo que proporciona una evidencia de auditoría con el mismo nivel de seguridad que la obtenida directamente por la confirmación del tercero.

---

dentro de una zona de códigos PDF 417.

Este procedimiento debe permitir revisar las cuentas de ingresos, gastos, inversiones o desinversiones mediante el contraste de la información obtenida directamente a través del sistema «SII», siempre que los clientes y proveedores se encuentren también incluidos dentro de este registro.