Guía práctica de fiscalización de los OCEX

GPF-OCEX 1503 La evidencia electrónica de auditoría

Referencia: NIA-ES-SP 1500

Documento elaborado por la Comisión Técnica de los OCEX y
aprobado por la Conferencia de Presidentes de la ASOCEX el 03/11/2022

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 (EEA), pero no establece ningún requerimiento adicional a las NIA-ES-SP.

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 mayoritaria.

En la presente revisión de la guía se han tenido en cuenta las NIA-ES más recientes, fundamentalmente la NIA-ES 315 (Revisada) y la NIA-ES 220 (Revisada), en lo referente a la evidencia de auditoría. Se ha reordenado parte del contenido de la guía respecto de la anterior versión de 20/05/2020 y se ha introducido un nuevo apartado 10 en línea con los pronunciamientos más recientes de IAASB.

En lo referente a la evidencia obtenida mediante el uso de herramientas y técnicas automatizadas debe consultarse la GPF-OCEX 5370.

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])*

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

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 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

La evidencia de auditoría es tanto la información y datos proporcionados por la entidad auditada como los obtenidos de terceros utilizada en la auditoría. También incluye los resultados de los procedimientos de auditoría (resultados de procedimientos sustantivos detallados y analíticos, procedimientos de valoración de riesgos y pruebas de controles).

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 y técnicas automatizadas (HTA). Mediante la realización de pruebas de controles.	En entornos complejos será indispensable la colaboración de especialistas en auditoría informática.

A su vez, la evidencia electrónica puede ser de dos tipos:

a) Información y datos almacenados en bases de datos y otro tipo de repositorios de la entidad auditada.

b) Procesos y controles implantados en los sistemas de información.

En 1998 las Normas de Auditoría del Sector Público de la IGAE ya distinguían entre ambos tipos de EEA y en su apartado 5.3.2, 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."*

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

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

La distinción entre ambos tipos de EEA resulta clara de la lectura de la Orden HAP/1781/2013 que se cita en el siguiente apartado (ver notas al pie).

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.

- 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

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."

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.

Hay que tener presente que los atributos de la EEA son diferentes de los de la evidencia tradicional en varios aspectos y eso afecta a los procedimientos de auditoría requeridos. En el siguiente cuadro se señalan las principales diferencias.[5] Las NIA-ES 315R y 330 abordan estas cuestiones tan relevantes en un entorno digital.

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.
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.

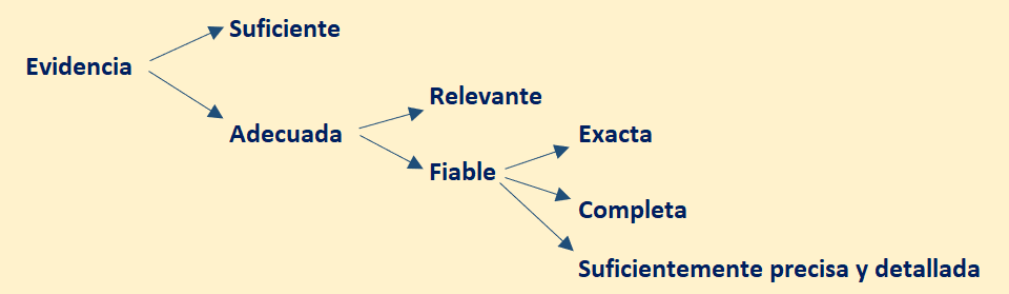
5 Véase: Émond, Caroline; Electronic Audit Evidence; The Canadian Institute of Chartered Accountants, 2003.

5. Características de la evidencia electrónica de auditoría

En la auditoría de cuentas anuales, la evidencia de auditoría debe tener unas características fundamentales para que el auditor pueda utilizarla como apoyo de sus conclusiones. De acuerdo con la NIA-ES-SP 1500:

> **El auditor diseñará y aplicará procedimientos de auditoría que sean adecuados, teniendo en cuenta las circunstancias, con el fin de obtener evidencia de auditoría suficiente y adecuada.**
>
> **Al realizar el diseño y la aplicación de los procedimientos de auditoría, el auditor considerará la relevancia y fiabilidad de la información que se utilizará como evidencia de auditoría.**

Es decir, la evidencia debe ser (ver apartados 6 a 9 de la NIA-ES-SP 1500):



La suficiencia es una medida cuantitativa de la evidencia de auditoría: la cantidad de evidencia de auditoría necesaria depende de la valoración del auditor del riesgo de incorrección material, así como de la calidad de dicha evidencia de auditoría (NIA-ES-SP 1500, p5.e).

La adecuación es una medida cualitativa de la evidencia de auditoría, es decir, su **relevancia** y **fiabilidad** para respaldar las conclusiones en las que se basa la opinión del auditor (NIA-ES-SP 1500, p5.b).

La **relevancia** se refiere a la conexión lógica con la finalidad del procedimiento de auditoría, o su pertinencia al respecto, y, en su caso, con la afirmación que se somete a comprobación.

Para que el auditor obtenga evidencia de auditoría **fiable**, la NIA-ES-SP 1500 (párrafo 9.a) exige a los auditores que obtengan evidencias sobre la **exactitud** y **completitud**[6] de la información generada por la entidad que vaya a utilizarse como evidencia de auditoría. La fiabilidad de la evidencia está influenciada por su fuente y naturaleza y depende de las circunstancias en que se obtenga. Con la evolución de la tecnología, hay múltiples fuentes de información disponible y algunas son más confiables que otras.

Además, la adecuación de la evidencia de auditoría obtenida dependerá de que la información sea **suficientemente precisa o detallada** para los fines del auditor.

La obtención de EEA 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 EEA 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.**

A fin de poder valorar la suficiencia y lo adecuado 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 completitud de la información. Los auditores deberían asegurar que los

[6] *Completeness* en el original en inglés, integridad en la NIA-ES-SP 1500.

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. 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.

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, duplicación, eliminación u ocultación.
- Las dificultades para comprobar la forma de su aprobación y firma, su autenticidad.

El equipo auditor al emplear evidencia, electrónica o analógica deberá garantizar su fiabilidad, además de asegurar que las tecnologías y aplicaciones empleadas para generar, transmitir, editar y almacenar la información son también confiables.

Cuando se utilicen herramientas y técnicas automatizadas (HTA) para analizar 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. En el apartado 14 de la GPF-OCEX 5370 se analiza con mayor exhaustividad esta cuestión cuando se utiliza HTA.

La evaluación de la exactitud y la completitud debe efectuarse tanto para la evidencia tradicional como para la obtenida mediante HTA. 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 una revisión de los CGTI y CPI**.

En cada caso se deberá analizar qué controles es preciso revisar para reforzar la fiabilidad de la EEA, dependiendo de las circunstancias y considerando los objetivos de los controles.

Desde el punto de vista del auditor, los objetivos de los CGTI (ver GPF-OCEX 5330) son proporcionar una garantía razonable de que los datos, la información y los activos de los sistemas de información cumplen las siguientes propiedades: confidencialidad, integridad, disponibilidad, autenticidad, y trazabilidad.

Objetivos de los CGTI	Descripción (según la GPF-OCEX 5330)
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 procesamiento de la información (**CPI)** y la realización de procedimientos sustantivos.

Los objetivos de los CPI son asegurar la completitud, exactitud, validez y legalidad de las transacciones y otra información:

Objetivos de los CPI	Descripción (según la GPF-OCEX 5340)
Completitud	Los controles de completitud proporcionan una seguridad razonable de que: - todas las transacciones reales son introducidas en el sistema, - si son válidas son aceptadas en el procesamiento, - son procesadas una sola vez, los duplicados son rechazados, - las transacciones rechazadas son identificadas, corregidas y reprocesadas; y - todas las transacciones aceptadas por el sistema son procesadas completamente. *Los controles más usuales son: totales de lotes, control de secuencia, control de duplicados, reconciliaciones, totalizadores e informes de excepción*.
Exactitud	Los controles de exactitud proporcionan una seguridad razonable de que: - las transacciones son registradas adecuadamente, con la fecha e importes correctos, en tiempo oportuno y en el periodo adecuado; - los datos son procesados de forma exacta por las aplicaciones, que producen resultados fiables con output exactos. *Se incluyen: validaciones, comprobaciones automáticas de razonabilidad, de dependencia, de existencia, de formato, de rangos, de exactitud matemática, etc.*
Validez	Los controles de validez proporcionan una seguridad razonable de que: - todas las transacciones registradas han ocurrido realmente, corresponden a la Entidad y han sido adecuadamente aprobadas; y de que - el output contiene solo datos válidos. Una transacción es válida cuando ha sido debidamente autorizada y cuando los datos maestros relativos a esa transacción son fiables (por ejemplo, los datos bancarios o domicilio del acreedor). La validez incluye el concepto de autenticidad. *Ejemplo: comprobar una factura con el pedido y el albarán de entrada antes de su aprobación.*
Legalidad	Los controles de legalidad proporcionan una seguridad razonable de que en la gestión de las operaciones se ha cumplido con la legalidad vigente.

8. 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 o revise ciertos controles sin apoyo de especialistas.

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

a) Revisando la información y bases de datos disponibles mediante pruebas realizadas con HTA.

Se hace necesario desarrollar nueva metodología de auditoría e introducir nuevas HTA 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, y 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 GPF-OCEX 1315R 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.**

9. 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 la información y 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 fuente de estos, dando implícitamente por supuesto que existen.

Cuando se actúa así, no se está aplicando un adecuado grado de escepticismo profesional, se está incurriendo en un riesgo importante de auditoría y se resiente la diligencia profesional exigida.

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 la extracción o 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 otro documento informático o la extracción 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.

10. El riesgo de exceso de confianza en la tecnología[7]

10.1 ¿Qué es?

Independientemente de que la entidad utilice la tecnología para proporcionar información, o de que el auditor utilice **herramientas y técnicas automatizadas (HTA)** para llevar a cabo los procedimientos de auditoría, el auditor debe ser consciente de ciertos **riesgos**.

[7] Este apartado está basado en "Material de apoyo relacionado con la tecnología. Preguntas frecuentes (FAQ) que abordan el riesgo de exceso de confianza en la tecnología: uso de herramientas y técnicas automatizadas y uso de la información producida por los sistemas de la entidad auditada", IAASB Technology FAQ, marzo de 2021

La nueva NIA-ES 220 Revisada señala en el apartado A34 que "*los impedimentos a la aplicación del escepticismo profesional en el encargo pueden incluir, entre otros, un* ***exceso de confianza en las herramientas y técnicas automatizadas,*** *que puede producir una falta de evaluación crítica de la evidencia de auditoría por el equipo del encargo*".

Continúa señalando en el apartado A35 que "*los* ***sesgos inconscientes o conscientes del auditor*** *pueden afectar a los juicios profesionales del equipo del encargo, incluido, por ejemplo, al diseñar y aplicar procedimientos de auditoría o en la evaluación de la evidencia de auditoría. Algunos ejemplos de sesgos inconscientes del auditor que pueden impedir aplicar el escepticismo profesional y, por lo tanto, afectar a la razonabilidad de los juicios profesionales del equipo del encargo en el cumplimiento de los requerimientos de esta NIA incluyen:*

- ***Riesgo de automatización****, que es la tendencia a dar preferencia a resultados generados por sistemas automatizados, incluso cuando el razonamiento humano o información contradictoria cuestionan la fiabilidad del resultado o su adecuación*."

Como consecuencia de ello, aumenta el riesgo de confianza excesiva en la información o en la tecnología.

Las Normas de Auditoría del Sector Público (5.3.10) de la IGAE[8] ya recogían 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.

Es decir, el uso de la tecnología puede crear **sesgos** o un **riesgo general de confianza excesiva** en la información o en los resultados del procedimiento de auditoría realizado.

El exceso de confianza puede deberse a distintas causas, tales como no entender un HTA que se está utilizando, o asumir que los resultados de un HTA, o el sistema de una entidad, son apropiados para su uso sin más consideración.

La excesiva confianza en la tecnología puede ser la causa o el resultado de una falta de escepticismo profesional o de juicio profesional. Hay varias medidas que el auditor puede considerar, y los OCEX pueden tomar para ayudar al auditor, para abordar los sesgos y el riesgo de una confianza excesiva.

10.2 ¿Cómo pueden los OCEX ayudar al auditor a abordar el sesgo de automatización y el riesgo de confianza excesiva al utilizar HTA?

Aplicar determinadas políticas o procedimientos

Los OCEX pueden disponer de políticas o procedimientos para asegurar que obtengan o desarrollen, apliquen, mantengan y utilicen adecuadamente los recursos tecnológicos en la realización de las auditorías[9]. Estas políticas o procedimientos pueden incluir las siguientes cuestiones:[10]

- El recurso tecnológico funciona como está diseñado y logra el propósito para el que está destinado.
- Los outputs de la aplicación de TI alcanzan el propósito para el que se utilizarán.
- La necesidad de conocimientos especializados para utilizar eficazmente los recursos tecnológicos, incluida la capacitación de las personas que utilizarán los recursos tecnológicos.
- La necesidad de desarrollar procedimientos que definan el funcionamiento del recurso tecnológico.

Los OCEX deben tener en cuenta las GPF-OCEX 1503 y 5370.

Los OCEX pueden considerar la posibilidad de elaborar una lista de recursos tecnológicos para los que se han aplicado las políticas o procedimientos mencionados dentro de los OCEX. Estos recursos pueden ser aprobados para su uso en los trabajos de auditoría, junto con el propósito específico de cada recurso. Los OCEX también pueden establecer políticas o procedimientos para hacer frente a las circunstancias cuando el equipo de

8 Resolución de 1 de septiembre de 1998.

9 NIGC1-ES "Gestión de la calidad en las firmas de auditoría que realizan auditorías de estados financieros", párrafo 32(f).

10 NIGC1-ES, párrafo A100

auditoría utilice un recurso tecnológico que no haya sido aprobado por el OCEX.[11]

Ejemplo de cómo las políticas o procedimientos de un OCEX ayudaron al auditor a abordar el riesgo de dependencia excesiva

El OCEX requiere documentar en una auditoría porqué un recurso tecnológico que no ha sido aprobado centralmente por el OCEX, es apropiado para usarse en la misma. La documentación incluirá:

- *Cómo ha determinado el equipo de auditoría que el HTA (recurso tecnológico) no estándar utilizado para llevar a cabo los procedimientos de auditoría es adecuado para su propósito;*
- *Si el equipo de auditoría tiene la competencia y las capacidades adecuadas para utilizar el HTA; y*
- *Si el HTA utilizado para llevar a cabo los procedimientos de auditoría está ejecutando la tarea prevista.*

Un miembro del equipo de auditoría obtiene una macro de hoja de cálculo de un miembro de otro equipo de auditoría para ayudar a valorar los activos intangibles. La macro no ha sido aprobada centralmente por el OCEX; por lo tanto, el miembro del equipo de auditoría completa la documentación requerida por el OCEX. A medida que el miembro del equipo de auditoría está tratando de completar la documentación, resulta evidente que no se comprende suficientemente cómo la macro está determinando el valor razonable del activo intangible y si la macro es adecuada para el propósito previsto. En consecuencia, el miembro del equipo reconoce que puede haber una confianza excesiva de la macro (de manera que se puedan adoptar nuevas medidas adecuadas).

Mejorar la formación

Los OCEX pueden considerar la posibilidad de incluir en su formación lo siguiente:

- «Consideraciones tecnológicas» para ilustrar que las normas se aplican por igual, tanto si se utilizan HTA como si no; sin embargo, también se destacan consideraciones especiales en la ejecución de las normas cuando se utiliza HTA.
- La importancia del escepticismo profesional al usar HTA y estar alerta al sesgo de automatización.
- Cuándo y cómo utilizar ciertos HTA en la realización de procedimientos de auditoría.

Concienciación

Además de la formación, los OCEX también pueden considerar métodos para crear concienciación sobre la posible confianza excesiva en las HTA y sugerencias sobre cómo hacer frente a su ocurrencia, tales como:

- Comunicar, por ejemplo, a través de las guías de auditoría, la importancia del escepticismo profesional cuando se utiliza HTA y el impacto que tiene en la calidad de la auditoría.
- Organizar campañas internas (para mostrar diversos aspectos de la calidad de las auditorías) y alentar al auditor a que se comprometa a aumentar la calidad de las auditorías, incluida una mayor concienciación de las repercusiones que tiene en la calidad una confianza excesiva de la tecnología.

10.3 ¿Cómo puede el auditor abordar el sesgo de automatización o el riesgo de confianza excesiva en la información proporcionada por el sistema automatizado de la entidad auditada?

Conocer los sesgos, reconocer la posibilidad de sesgos y reconocer sus causas son los primeros pasos para abordarlos. **Mantenerse alerta sobre los sesgos y mantener el escepticismo profesional al realizar la auditoría, incluida la evaluación crítica de la evidencia de auditoría, ayudará al auditor a abordar el riesgo de sesgo al examinar la información producida por el sistema automatizado de la entidad**.

Entre las medidas que el auditor puede adoptar para hacer frente al riesgo de sesgo de automatización o al riesgo de confianza excesiva en la información producida por los sistemas de la entidad figuran las siguientes:

- Alertar explícitamente al equipo de auditoría sobre casos o situaciones en que la vulnerabilidad al sesgo de automatización puede ser mayor y hacer hincapié en la importancia de recabar asesoramiento de miembros más experimentados del equipo de auditoría para planificar y llevar a cabo los procedimientos de auditoría.

[11] NIGC1-ES, párrafo A101

Ejemplo:

Durante las deliberaciones del equipo de auditoría, en la reunión para discutir los riesgos, los miembros más experimentados del equipo destacaron que la entidad había implantado un nuevo sistema de costes para hacer un seguimiento de los costes reales de las materias primas que el equipo de auditoría utilizaba para las pruebas de valoración de los inventarios.

Los miembros del equipo debatieron explícitamente cómo la vulnerabilidad al sesgo de automatización podría ser mayor en esta situación porque la entidad indicó que el sistema se había desarrollado específicamente con el fin de hacer un seguimiento de los costos reales y se había puesto a prueba a fondo.

Se recordó a los miembros del equipo los requisitos relativos a la información producida por la entidad en la NIA-ES-SP 1500 y GPF-OCEX 1503. Los miembros del equipo también hicieron hincapié en la importancia de buscar asesoramiento TI.

- Implicar a los miembros del OCEX con conocimientos y habilidades especializados o a expertos externos para ayudar al equipo de auditoría en áreas complejas de la auditoría.
- Modificar la naturaleza, el momento y la extensión de la dirección, la supervisión o las revisiones mediante la participación de miembros del equipo con más experiencia, una supervisión sobre una base más frecuente o exámenes más a fondo.
- Evaluar si la información es suficientemente fiable, incluida, entre otros factores, la obtención de pruebas de auditoría sobre la exactitud y completitud de las entradas de datos en los sistemas de la entidad (véase más adelante el análisis de la NIA-ES-SP 1500).

Además, el cumplimiento de las NIA-ES-SP y GPF-OCEX también ayuda al auditor a abordar el riesgo de sesgo de automatización y confianza excesiva de la información producida por los sistemas de la entidad, por ejemplo:

- La NIA-ES-SP 1200 exige que el auditor ejerza un juicio profesional en la planificación y realización de una auditoría, y que planifique y lleve a cabo una auditoría con escepticismo profesional, reconociendo que pueden existir circunstancias que hagan que los estados financieros contengan incorrecciones materiales.[12] En el contexto de la excesiva confianza en la información producida por los sistemas de la entidad, es importante que el auditor mantenga una mente interrogante y evalúe críticamente las evidencias, incluso si se relaciona con información procedente de un sistema automatizado.

  Además, el ejercicio del juicio profesional se reitera en todas las NIA-ES-SP, lo que recuerda al auditor que se requiere un juicio profesional durante toda la auditoría.

- El apéndice 5 de la NIA-ES 315R proporciona orientación sobre el conocimiento del uso de TI por la entidad en los componentes del sistema de control interno. En el apéndice 6 se exponen consideraciones para conocer los CGTI. Estos apéndices ayudan al auditor a comprender el uso de la tecnología por parte de la entidad, reduciendo así el riesgo de dependencia excesiva de la información producida por los sistemas de la entidad al realizar los procedimientos de auditoría.

  Los OCEX deben aplicar la GPF-OCEX 1315R.

- La NIA-ES-SP 1500 exige al auditor que considere la pertinencia y fiabilidad de la información que debe utilizarse como prueba de auditoría.[13] Al utilizar la información producida por la entidad, la NIA-ES-SP 1500 también requiere que el auditor, según sea necesario en las circunstancias, obtenga **pruebas de auditoría sobre la exactitud y exhaustividad de la información y evalúe si la información es suficientemente precisa y detallada a los efectos del auditor**.[14]

  Tanto si se trata de tecnología como si no, el ejercicio del escepticismo profesional puede incluir la consideración de la suficiencia y la idoneidad de las pruebas de auditoría a la luz de las circunstancias, lo que ayuda a reducir el riesgo de que el auditor dependa de cualquier información en particular, como

[12] NIA-ES-SP 1200, *Objetivos generales del Auditor Independiente y la realización de una auditoría de conformidad con las Normas Internacionales de Auditoría*, párrafos 15 a 16

[13] NIA-ES-SP 1500, párrafo 7

[14] NIA-ES-SP 1500, párrafo 9

información de Internet, extractos de datos de sistemas de las entidades auditadas, informes generados por sistemas o cuadros de mando y previsiones preparadas por las entidades auditadas.

Los OCEX deben considerar también la GPF-OCEX 1503 La evidencia electrónica de auditoría.

10.4 ¿Cómo puede el auditor abordar el sesgo de automatización y el riesgo de confianza excesiva cuando utiliza sus propias HTA?

Comprender el sesgo de automatización y reconocer su posibilidad y sus causas es el primer paso para abordarlo. Las acciones que el auditor puede tomar para mitigar el riesgo de sesgo de automatización al utilizar sus propias HTA incluyen:

- Alertar explícitamente al equipo de auditoría sobre casos o situaciones en que la vulnerabilidad al sesgo de automatización puede ser mayor.
- Haciendo hincapié en la importancia de recabar asesoramiento de los miembros más experimentados del equipo para planificar y llevar a cabo los procedimientos de auditoría.

> *Ejemplo de búsqueda de consejo de los miembros más experimentados*
>
> *El auditor de una gran entidad utiliza una herramienta automatizada de prueba de asientos de diario. La herramienta está programada para analizar todos los asientos, y extrae los que siguen 50 rutinas comunes para que el auditor los considere (por ejemplo, asientos hechos los fines de semana, que terminan en 999 etc.).*
>
> *Reconociendo el potencial de sesgo de automatización (que en esta circunstancia estaría ejecutando las 50 rutinas de entrada de asientos sin consideración), el auditor busca el asesoramiento de un miembro del equipo más experimentado. Consideran cuál de las 50 rutinas es aplicable a la entidad (por ejemplo, «entradas hechas en un fin de semana» no es una característica de alto riesgo, ya que las entradas de venta se publican automáticamente, y el centro está abierto los fines de semana; sin embargo, los asientos que terminan en 999 o 000 serían bastante inusuales). Además, recuerdan que el centro está cerrado en diciembre y enero, y por lo tanto las entradas de ingresos hechas en esos dos meses deben ser seleccionadas para las pruebas de asientos. El auditor diseña su propia rutina en la herramienta para seleccionar esos asientos.*

- Involucrar a miembros del equipo con habilidades y conocimientos especializados, o a un experto externo, para ayudar al equipo de auditoría en áreas complejas o subjetivas de la auditoría.

Además, el cumplimiento de las NIA-ES-SP y las GPF-OCEX también ayuda al auditor a abordar el riesgo de sesgo de automatización y la confianza excesiva de la tecnología cuando utiliza sus propias HTA, por ejemplo:

- La NIA-ES 220 (Revisada) exige que los responsables de los equipos asuman la responsabilidad de utilizar los recursos de manera adecuada.[15] Las políticas o procedimientos del OCEX pueden ayudar a este respecto, ya que esos procedimientos pueden ayudar a evitar que el equipo de auditoría dependa indebidamente de la suposición de que los resultados de las HTA son siempre exactos o apropiados (véase el punto 2).
- La NIA-ES-SP 1330 requiere que el auditor diseñe y lleve a cabo procedimientos de auditoría que respondan a los riesgos valorados de incorrección material.[16] En consecuencia, el auditor tal vez deba considerar si sus respuestas y procedimientos (incluido el uso del HTA) abordan los riesgos valorados de incorrección material, reduciendo así el riesgo de que el auditor se base en un procedimiento en particular.

La aplicación del juicio profesional ayuda al auditor a abordar la confianza excesiva. **El auditor está obligado a** ejercitar un juicio profesional durante toda la auditoría, por ejemplo, al determinar:

- La materialidad;
- Valoración de los riesgos;

[15] NIA-ES 220 (revisada), párrafo 28

[16] NIA-ES-SP 1330, *Respuestas del auditor a los riesgos valorados,* párrafos 5 a 6

- La naturaleza, el momento de realización y la extensión de los procedimientos de auditoría;
- Si es necesario seguir trabajando para alcanzar los objetivos de las NIA-ES-SP;
- La evaluación de las decisiones de la dirección en la aplicación del marco de información financiera aplicable de la entidad; y
- La razonabilidad de las estimaciones hechas por la administración en la preparación de los estados financieros.

Las HTA están disponibles para ayudar al auditor en las esferas mencionadas. Sin embargo, la opinión profesional del auditor sigue siendo necesaria para complementar los resultados de las HTA, por ejemplo:

El auditor utiliza una herramienta para calcular la materialidad utilizando la información financiera de la entidad y el sector en el que opera la entidad. La herramienta aplica un punto de referencia predeterminado basado en la selección del sector y porcentajes predeterminados dado el punto de referencia.

Se requiere juicio profesional para determinar (o acordar) el punto de referencia de la herramienta, y determinar el porcentaje apropiado para aplicar al punto de referencia, ya que el auditor puede ser consciente de otros factores que pueden no haber sido considerados por el punto de referencia preestablecido y los porcentajes utilizados por la herramienta, como la forma en que la entidad es financiada o su estructura de propiedad.

El auditor utiliza una herramienta para analizar la información financiera de la entidad a fin de determinar los saldos materiales, las correlaciones irregulares (por ejemplo, aumento de los ingresos pero disminución de las cuentas por cobrar) y las grandes fluctuaciones para detectar posibles riesgos de incorrección material.

Se requiere juicio profesional para determinar si existe un riesgo de incorrección material porque puede haber otras circunstancias que a herramienta no haya tenido en cuenta (como controles ineficaces o un elevado volumen de trabajo en el departamento de contabilidad) que pueden sugerir riesgos adicionales de incorrección material.

11. 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.

Control de versiones

Versión	Cambios
20/05/2020	Versión inicial aprobada por la Conferencia de Presidentes de ASOCEX.
03/11/2022	Se actualiza el apartado 1. Se ha reordenado todo el contenido de la guía y sus anexos de una forma más sistemática. Se han ampliado los apartados 5 y 7 en coherencia con las nuevas NIA-ES 220R, GPF-OCEX 1315R y GPF-OCEX 5370. Se añade un nuevo apartado "10. El riesgo de exceso de confianza en la tecnología".

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[17].Se admitirán como **sistemas de firma**[18]:

- 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
- 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

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

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

- la identificación de los usuarios y el control de accesos
- el cumplimiento de las garantías previstas en la legislación de protección de datos.

2. Documentación de la evidencia electrónica de auditoría

2.1 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.

2.2 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.

2.3 Trabajo de análisis de datos realizado con HTA

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*.

3. Ejemplos de nuevas evidencias electrónicas

3.1 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[19].

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

- 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[20].

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

20 *¿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.

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[21].

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.

¿Qué se entiende por unidad tramitadora?

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

21 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 dentro de una zona de códigos PDF 417.