Guía práctica de fiscalización de los OCEX

GPF-OCEX 5370 Guía para la realización de pruebas de datos

Referencia: NIA-ES 315 (Revisada) y GPF-OCEX 1315 (Revisada)

Documento elaborado por la Comisión Técnica de los OCEX y
aprobado por la Conferencia de Presidentes de ASOCEX el 03/11/2022. *Corrección de errores de 19/10/2023.*

I INTRODUCCIÓN Y ASPECTOS GENERALES

1. Introducción y objetivos de esta guía

2. Las herramientas y técnicas automatizadas: definición y tipos

3. Uso de HTA/ADA en la valoración de riesgos y como procedimiento de auditoría posterior

4. Ejercicio del escepticismo profesional al utilizar HTA

5. Uso del análisis de datos (ADA) en la auditoría

6. Ventajas y limitaciones del uso del análisis de datos (ADA)

7. Etapas para la realización de una prueba de datos

II LA PLANIFICACIÓN DE UNA PRUEBA DE DATOS

8. ¿Cómo afecta a las actividades de planificación el posible uso de HTA en una auditoría?

9. Planificación y diseño de las pruebas de datos (ADA)

10. El documento de inicio de la auditoría (DIA) y la solicitud de la información

11. Formato de los datos solicitados

III ACCESO Y EXTRACCIÓN DE LOS DATOS

12. Criterios generales para la obtención de la información necesaria para realizar una prueba de datos

13. Procedimientos de obtención de la información para realizar una prueba de datos

14. Obtención de la información mediante acceso directo a la base de datos

15. Garantizar la fiabilidad de los datos en el proceso de su obtención y transformación

16. ¿Dónde se almacenarán los datos obtenidos y cómo se mantendrá su integridad?

IV DISEÑO Y EJECUCIÓN DE LAS PRUEBAS

17. Archivo de la información recibida (ejemplo con ACL)

18. Codificación de la prueba

19. Automatización de las pruebas: Scripts

20. Análisis de los resultados obtenidos y conclusiones

V DOCUMENTACIÓN DE LAS PRUEBAS

21. Introducción. El uso de HTA y la documentación del auditor

22. Contenido de la documentación de una prueba de datos

ANEXOS ver documento separado

La presente guía, preparada por la Comisión Técnica de los OCEX, es un compendio de lo establecido en las distintas normas de auditoría que se citan posteriormente, relacionado con el uso de herramientas y técnicas automatizadas (HTA) en la ejecución de auditorías, de la literatura técnica internacional más reciente y de la experiencia práctica de los OCEX a lo largo de los años.

*El objetivo número uno es servir de ayuda a los equipos de auditoría en la utilización de estas HTA, exponiendo tanto los fundamentos conceptuales como la exposición detallada de los procedimientos principales para el uso de las HTA incluyendo ejemplos prácticos. El resultado ha sido inevitablemente extenso, pero no hemos querido separar ambos enfoques ya que los consideramos complementarios para la adecuada comprensión de un tipo de herramientas y técnicas cada vez más necesarias, si no **indispensables**, en la fiscalización en entornos de administración electrónica avanzada.*

*Por esta razón es recomendable la lectura de esta guía a **auditores sin experiencia** en el uso de HTA, que podrán centrarse en los capítulos más generales e introductorios para progresar paulatinamente con la práctica. Pero también es recomendable para los **auditores con conocimientos avanzados** ya que se tratan cuestiones que requieren un alto nivel de conocimientos teóricos y prácticos.*

I INTRODUCCIÓN Y ASPECTOS GENERALES

1. Introducción y objetivos de esta guía

La nueva ***NIA-ES 220 (Revisada) Gestión de la calidad de una auditoría de estados financieros***[1] señala que

> "La utilización de **recursos tecnológicos** en una auditoría **puede ayudar al auditor en la obtención de evidencia de auditoría suficiente y adecuada**. Las herramientas tecnológicas pueden permitir que el auditor gestione la auditoría de un modo **más eficaz y eficiente**.
>
> Las herramientas tecnológicas también pueden permitir que el auditor evalúe **grandes cantidades de datos** con más facilidad para, por ejemplo, proporcionarle información con mayor profundidad, identificar tendencias inusuales o cuestionar más eficazmente las afirmaciones de la dirección, lo que mejora la capacidad del auditor para aplicar el escepticismo profesional.
>
> Las herramientas tecnológicas también se pueden utilizar para realizar reuniones y proporcionar **herramientas de comunicación** al equipo de *auditoría*.
>
> La **utilización inadecuada** de esos recursos tecnológicos puede, sin embargo, incrementar el **riesgo de un exceso de confianza** en la información generada para la toma de decisiones, o puede originar amenazas para el cumplimiento de los requerimientos de ética aplicables, por ejemplo, de los requerimientos relacionados con la **confidencialidad**".

Recursos tecnológicos es un concepto amplio que incluye todo tipo de elementos a disposición de los auditores para llevar a cabo sus tareas, tales como software para gestionar los papeles de trabajo (como TeamMate), ofimático (Word, Excel, etc.), trabajo en equipo (Teams, Slack) o las herramientas y técnicas automatizadas que se comentan a continuación.

Debido a la creciente e imparable utilización de herramientas y técnicas automatizadas en la realización de procedimientos de auditoría, la NIA-ES 315R[2] trata diferentes aspectos de su uso en varios apartados específicos titulados "Herramientas y técnicas automatizadas" (ver ***Anexo 1 La NIA-ES 315 (revisada) y las herramientas y técnicas automatizadas***).

Adicionalmente, dada la importancia que está adquiriendo en la actividad auditora la utilización de HTA, la IAASB[3] ha emitido una serie de guías orientativas (***IAASB Technology Focus Area***) sobre su utilización por el auditor en el marco de las NIA. Dichas publicaciones, junto con otro material recientemente publicado y la experiencia práctica de los OCEX, se han utilizado para actualizar la GPF-OCEX 5370 (2018).

Esta guía intenta ser coherente con las NIA-ES-SP y las GPF-OCEX de aplicación en los OCEX y, en caso de discrepancia, prevalecerán las NIA-ES-SP o las GPF-OCEX que las sustituyan.

En la literatura técnica previa a la NIA-ES 315R se utilizaba con frecuencia la denominación "*técnicas de auditoría asistidas por ordenador" (CAAT).* Por razones de uniformidad en la utilización de la terminología, a partir de ahora utilizaremos, de acuerdo con la citada NIA-ES 315R, la expresión genérica de **herramientas y técnicas automatizadas (HTA)** cuando nos refiramos a un amplio espectro de herramientas o técnicas, y utilizaremos la más específica de **análisis de datos de auditoría (ADA**) cuando realicemos las habituales **pruebas de datos** con herramientas tales como ACL, IDEA, Tableau, Excel u otras herramientas similares.

El objetivo de esta guía es ayudar al auditor a entender qué son las herramientas y técnicas automatizadas (HTA), qué tipos hay y cuáles son sus posibles usos durante la realización de una auditoría en un entorno de administración electrónica avanzada.

---

1 Apartado A63 de la NIA-ES 220 (Revisada) (ver Resolución de 2 de febrero de 2022, del ICAC).

2 Aprobada mediante Resolución de 14 de octubre de 2021, del Instituto de Contabilidad y Auditoría de Cuentas, y recogida en la **GPF-OCEX 1315 Revisada**. Todas las referencias realizadas a la NIA-ES 315R deben entenderse realizas también a la GPF-OCEX 1315R.

3 International Auditing and Assurance Standards Board.

De una forma más detallada, la finalidad de la guía es:

- **Informar sobre la utilización de las herramientas y técnicas automatizadas en las auditorías y sobre las normas técnicas de auditoría aplicables.**
- **Establecer criterios homogéneos y metodologías comunes para la realización de las pruebas de datos para todos los auditores de los OCEX.**
- **Asegurar la adecuada planificación y realización de las pruebas, evitando retrasos que afecten a la buena marcha del trabajo y errores en la ejecución de las pruebas.**
- **Proporcionar información al auditor sobre las posibles formas de extracción de los datos, con el fin de que pueda utilizar el mecanismo de obtención de datos más adecuado en función de las características específicas de la auditoría y de las pruebas a realizar.**
- **Estandarizar los distintos procedimientos para la obtención de datos.**
- **Garantizar que la fuente de datos y los datos obtenidos con fiables y completos.**
- **Asegurar la generación de evidencia de auditoría suficiente y adecuada en las pruebas de datos.**
- **Asegurar la adecuada documentación de las pruebas, de forma estandarizada.**
- **Automatizar en la medida de lo posible la ejecución de las pruebas de datos, con el objetivo de incrementar la eficiencia en su ejecución.**
- **Generar un fondo documental de conocimiento en los OCEX para la realización de las pruebas de datos de las entidades fiscalizadas en beneficio de fiscalizaciones subsiguientes.**

El cumplimiento de esta guía de auditoría permitirá alcanzar altos niveles de **calidad** en todo el proceso. **El auditor responsable de la auditoría debe asegurarse de que se siguen sus criterios en todo momento**.

2. Las herramientas y técnicas automatizadas: definición y tipos[4]

Los procedimientos de auditoría pueden llevarse a cabo utilizando una serie de herramientas[5] o técnicas[6], que pueden ser manuales o automatizadas o una combinación de ambas.

Aunque el término «análisis de datos» se utiliza en ocasiones para referirse a tales herramientas y técnicas, el término no tiene una definición o descripción uniforme. Este término es demasiado limitado porque no abarca todas las tecnologías emergentes que se están utilizando al diseñar y llevar a cabo los procedimientos de auditoría en la actualidad. Por esta razón, en la NIA-ES 315R se utiliza el término más amplio de herramientas y técnicas automatizadas (HTA).

Las HTA engloban herramientas y técnicas de distinta naturaleza, incluido el análisis de datos mediante modelización y visualización, automatización de procesos robóticos, inteligencia artificial y aprendizaje automático, y tecnología de drones para observar o inspeccionar activos[7]. El uso de tales herramientas y técnicas automatizadas puede complementar o reemplazar tareas manuales o repetitivas.

En definitiva, a los efectos de una auditoría, las HTA consisten en el uso de herramientas TI para llevar a cabo procedimientos de auditoría, lo que conlleva la automatización de estos.

En ciertas circunstancias, un auditor puede considerar que el uso de HTA para llevar a cabo determinados procedimientos de auditoría puede dar lugar a evidencias de auditoría más convincentes en relación con la afirmación que se está comprobando (*por ejemplo, cuando se audite una entidad grande que opera en un entorno de administración electrónica avanzada*). En otras circunstancias, la realización de procedimientos de auditoría puede ser eficaz sin el uso de HTA e incluso resultar más apropiado, en términos de eficiencia, no utilizarlas (*por ejemplo, cuando se audite una entidad pequeña, con poco personal y procesos sencillos y manuales*).

---

4 La fuente principal de este apartado son los documentos de IAASB Technology Focus Area.

5 Las **herramientas** son el *software* que permite realizar los tratamientos de los datos precisos para ejecutar las pruebas de auditoría. Por ejemplo, Excel, Access, Power BI, Power Pivot, ACL, IDEA, Tableau, SAS, etc.

6 **Técnicas** son las diferentes formas en que se accede, se organizan, se analizan los datos y se comunican los resultados.

7 NIA-ES 315 (revisada), apartado A35.

Al aplicar las NIA-ES-SP, un auditor puede diseñar y realizar procedimientos de auditoría de forma tradicional o mediante el uso de HTA, y cualquier técnica puede ser eficaz. **Independientemente de las herramientas y técnicas utilizadas, el auditor debe cumplir con las NIA-ES-SP**.

Entre los **tipos de herramientas y técnicas automatizadas** que pueden utilizarse para llevar a cabo los procedimientos de auditoría cabe citar los siguientes:

- **Análisis de datos (ADA)**[8]: utilizados para evaluar conjuntos completos de datos mediante el descubrimiento y análisis de patrones y tendencias, la identificación e investigación de elementos inusuales, desviaciones y anomalías. También puede utilizarse para la identificación y valoración de riesgos de incorrección material que pueden no haber sido tan fácilmente visibles o evidentes mediante el uso de procedimientos más tradicionales. En esta guía nos referiremos básicamente a este tipo de técnicas y herramientas, a las que también denominamos, de forma indistinta, como **pruebas de datos**.
- **Automatización robótica de procesos (RPA)**: consiste en el procesamiento de datos estructurados mediante un software que automatiza las actividades que los seres humanos realizan, tareas típicamente repetitivas que requieren un juicio mínimo. *Por ejemplo, la RPA se puede utilizar para realizar el análisis del libro mayor general e identificar asientos que no cuadran, están duplicados, están por encima de un umbral definido o muestran ciertas características o para automatizar la carga de datos, verificar su integridad y ejecutar pruebas estándar, como muestreos.*
- **Técnicas de inteligencia artificial**: tecnología de aprendizaje automático configurada para reconocer patrones en grandes volúmenes de datos, incluidos datos no estructurados como correos electrónicos, contratos, facturas, imágenes y archivos de audio de reuniones. Los auditores pueden utilizar la inteligencia artificial para reunir información de diversas fuentes y determinar los riesgos de incorrecciones materiales.

3. Uso de HTA/ADA en la valoración de riesgos y como procedimiento de auditoría posterior

Los auditores pueden utilizar HTA/ADA en un procedimiento de auditoría para procesar, organizar, estructurar o presentar datos a fin de generar información que pueda utilizarse como evidencia de auditoría. Tanto los procedimientos de valoración de riesgos como los procedimientos de auditoría posteriores proporcionan evidencias de auditoría.

a) Procedimientos de valoración de riesgos

Las HTA/ADA pueden utilizarse en el análisis de datos para identificar o evaluar los riesgos de inexactitudes materiales. Esto puede hacerse mediante la identificación de incoherencias, transacciones inesperadas, eventos, cantidades, ratios y tendencias. Las HTA/ADA pueden brindar al auditor la oportunidad de procesar grandes conjuntos de datos y considerar también datos de una variedad de fuentes. Al hacerlo, el auditor puede obtener una comprensión más profunda y detallada de las características o la composición de la población, incluida la naturaleza y el alcance de los acontecimientos o condiciones que pueden dar lugar a

[8] NIA-ES 315 (revisada), apartado A31.

riesgos de incorrecciones materiales. Este conocimiento puede ayudar a identificar hechos o condiciones que afecten la susceptibilidad a la incorrección de una clase o tipo de transacciones, el saldo de la cuenta o la divulgación, o proporcionar más información para fundamentar la valoración de los riesgos identificados.

Cuando se llevan a cabo procedimientos de valoración de riesgos de conformidad con la NIA-ES 315R, las HTA pueden ayudar al auditor a comprender la estructura institucional y operativa de una entidad y a comprender los flujos de transacciones y su procesamiento como parte de los procedimientos para comprender el sistema de información (*NIA-ES 315R, apartado A57*).

En el ***Anexo 3 Uso de HTA/ADA en la valoración de riesgos*** se ponen ejemplos de cómo utilizar las HTA/ADA en los procedimientos de valoración de riesgos de acuerdo con la NIA-ES 315R.

b) Procedimientos de auditoría posteriores

Según el apartado A10.b) de la NIA-ES-SP 1500, los procedimientos de auditoría posteriores comprenden:

(i) **Pruebas de controles**, cuando las requieran las NIA-ES-SP o cuando el auditor haya decidido realizarlas; y

(ii) **Procedimientos sustantivos**, que incluyen **pruebas de detalle** y **procedimientos analíticos sustantivos**.

La realización de procedimientos analíticos sustantivos (PAS) generalmente es más aplicable a grandes volúmenes de transacciones que tienden a ser previsibles a lo largo del tiempo *(NIA-ES-SP 1520, párrafo A6)*. La evolución de la tecnología, junto con el aumento en el número y la variedad de fuentes de datos, puede crear más oportunidades para que el auditor utilice HTA en la realización de PAS.

Al aplicar los requisitos de NIA-ES-SP 1520 relativos al diseño y el rendimiento de PAS, hay ciertas consideraciones específicas para el uso de HTA:

a) Evaluación de la fiabilidad de los datos cuando se utiliza HTA

b) Evaluación de la precisión de la expectativa cuando se utiliza HTA

c) Otras consideraciones en la aplicación de los requisitos de la NIA-ES-SP 1520

En el ***Anexo 4 Uso de HTA/ADA como procedimiento de auditoría posterior*** se muestran ejemplos de estas cuestiones.

En algunos casos, el auditor puede utilizar el mismo ADA y los mismos datos para lograr el objetivo de más de un tipo de procedimiento de auditoría. Se pueden llevar a cabo procedimientos de auditoría como parte de la identificación y valoración de los riesgos de incorrección material (es decir, un procedimiento de valoración de riesgos[9]) que también son capaces de detectar incorrecciones materiales a nivel de afirmación, cumpliendo así la definición de procedimiento sustantivo[10] (es decir, una categoría de procedimiento de auditoría posterior). En el **Anexo 4** se realizan diversas consideraciones sobre esta cuestión.

4. Ejercicio del escepticismo profesional al utilizar HTA

La NIA-ES-SP 1200[11] requiere que el auditor planifique y lleve a cabo la auditoría con **escepticismo profesional**, reconociendo que pueden existir circunstancias que hagan que los estados financieros contengan incorrecciones materiales. Es una actitud que implica una mentalidad inquisitiva, estar alerta a circunstancias que pueden indicar una posible incorrección por error o fraude, y una evaluación crítica de la evidencia.[12]

El auditor siempre debe aplicar el escepticismo profesional, con independencia de que en la auditoría se utilicen HTA o se realicen procedimientos de auditoría más tradicionales. En este sentido, cuando el auditor emplea HTA debe tener presente sus implicaciones y riesgos, entre los que se encuentran las siguientes:

- La complejidad de las pruebas o de las herramientas puede anular o reducir el nivel de supervisión necesario en el proceso de auditoría.

9 NIA-ES 315 (revisada), Identificación y valoración de los riesgos de incorrecciones materiales, párrafo 12 j)

10 NIA-ES-SP 1330, Respuestas del auditor a los riesgos valorados, párrafo 4 a)

11 NIA-ES-SP 1200, párrafo 15

12 NIA-ES-SP 1200, párrafo 13 (l)

- El uso de algoritmos sin analizar su efecto en los resultados puede condicionar las conclusiones, incluso hasta el punto de obtener conclusiones erróneas.
- La fiabilidad e integridad de los datos utilizados cuando se emplean HTA es un punto crítico que debe ser evaluado cuidadosamente.
- A medida que la tecnología sigue evolucionando, es importante evitar la **excesiva confianza** en el uso de HTA o en sus resultados. Por muy poderosas que sean estas herramientas, no son un sustituto del conocimiento y el juicio profesional del auditor (véase el apartado 10 de la GPF-OCEX 1503).

  Por ejemplo, las HTA pueden utilizarse para analizar los datos a fin de identificar patrones, correlaciones y fluctuaciones en relación con la información financiera producida por la entidad. Este análisis, enmarcado en el proceso de identificación y valoración de los riesgos de incorrecciones materiales, permite al auditor verificar que la evidencia de auditoría no esté sesgada para corroborar la existencia de riesgos de incorrecciones materiales o de que pueda ser contradictoria con la existencia de tales riesgos.

Es necesario analizar la lógica de los resultados del uso de HTA desde el conocimiento y perspectiva del auditor sobre el proceso y de la entidad auditados.

El ejercicio de escepticismo profesional sigue siendo necesario para evaluar críticamente la calidad y fiabilidad de los datos, así como los resultados de la utilización de herramientas y técnicas automatizadas.

Demostrar el ejercicio del escepticismo profesional al utilizar herramientas y técnicas automatizadas no es diferente a su demostración cuando se realizan otros tipos de procedimientos de auditoría.

La NIA-ES 315R explica que la documentación de diversos asuntos requeridos por la norma puede proporcionar evidencia del ejercicio de escepticismo profesional por parte del auditor. Esto incluye, por ejemplo, documentar cómo se llevó a cabo el procedimiento y cómo se evaluó la evidencia de auditoría del procedimiento de valoración del riesgo, incluida la documentación de cualquier juicio profesional.

Aunque el auditor pueda tener acceso a una amplia gama de datos, incluso de diversas fuentes (es decir, un aumento de la **cantidad**), el uso del juicio y el ejercicio de escepticismo profesional sigue siendo necesario para evaluar críticamente la **calidad y fiabilidad de los datos**, los resultados de la utilización de herramientas y técnicas automatizadas, así como el cuestionamiento de las pruebas de auditoría contradictorias obtenidas[13]. En el apartado 10 de la GPF-OCEX 1503 se profundiza en esta cuestión.

5. Uso del análisis de datos (ADA) en la auditoría

Cuando hablamos de la aplicación de ADA en la auditoría, estamos hablando de aplicar un procedimiento de auditoría que permita al auditor obtener evidencia de auditoría suficiente y adecuada para reducir el riesgo de auditoría a un nivel aceptablemente bajo y, en consecuencia, para permitirle llegar a conclusiones razonables en las que basar su opinión o conclusiones.

Los principales **tipos de pruebas** que se pueden llevar a cabo mediante el uso de ADA son:

- ✓ Análisis de patrones
- ✓ Visualización de datos
- ✓ Minería de procesos
- ✓ Análisis de segregación de funciones
- ✓ Pruebas de controles.
- ✓ Pruebas sustantivas.
- ✓ …..

Puede verse un mayor detalle en el ***Anexo 2 Ejemplos de tipos de pruebas que se pueden llevar a cabo mediante el uso de HTA/ADA***.

[13] NIA-ES-SP 1500, párrafo 7

Estas técnicas pueden aplicarse durante las distintas etapas de planificación y ejecución de la auditoría, y en todo tipo de procedimientos cuya finalidad y extensión de uso puede ser muy variada:

- Durante la fase de **planificación**, pueden ayudar en la obtención y análisis de la información disponible. Esto incluye conocer el flujo de información del proceso auditado y el análisis de los riesgos, el cual ayuda a la definición de la naturaleza, momento y extensión de las pruebas de auditoría.
- Durante la fase de **ejecución**, pueden ayudar a la recolección de información del sistema de gestión o de información financiera del auditado, a la evaluación del nivel de control interno y a la ejecución de pruebas sustantivas y de controles.
- Durante la redacción del **informe** de fiscalización, pueden ayudar al auditor a soportar y presentar mejor los hallazgos más relevantes y las conclusiones.

En definitiva, utilizar ADA es muy útil en aquellos casos en los que un volumen importante de datos de una entidad auditada está disponible en formato electrónico. **En un entorno de administración electrónica los datos solo estarán disponibles en este formato**, por lo que en estos entornos utilizar ADA **resulta imprescindible para obtener evidencia suficiente y adecuada** en las auditorías financieras y de cumplimiento.

6. Ventajas y limitaciones del uso del análisis de datos (ADA)

Ventajas. Las ventajas que proporciona la realización de pruebas de datos con estas herramientas son:

a) **Mejora de la capacidad del auditor para obtener evidencia** de auditoría a partir del análisis de poblaciones más grandes, incluso del 100%, permitiendo mejores selecciones basadas en el riesgo de esas poblaciones para que el auditor haga pruebas más a fondo. Al permitir en muchos casos el análisis de la totalidad de los elementos y eliminar, por lo tanto, el riesgo de muestreo, las conclusiones resultan más objetivas.

b) **Automatización y repetición**. Aumenta la efectividad y eficiencia, proporcionando por tanto un ahorro de tiempo a considerar y facilita la escalabilidad de las pruebas.

c) **Seguridad** en la manipulación de los datos originales, que no pueden alterarse erróneamente, utilizando herramientas especializadas (ACL/IDEA).

d) **Una visión y comprensión más amplia y profunda** de la entidad y su entorno por parte de los auditores. En un entorno de administración electrónica avanzada, cada vez más complejo y con grandes volúmenes de datos, el uso de la tecnología ofrece oportunidades para que el auditor obtenga una comprensión más efectiva y completa de la entidad y su entorno, mejorando la calidad de la valoración de los riesgos y las respuestas del auditor. Esto también posibilita la mejora de las comunicaciones con los responsables de la entidad.

e) Más facilidades en la aplicación del **juicio y el escepticismo profesional**, ya que tiene acceso a más información y más desagregada, lo que permite afinar más en las tendencias y, por tanto, en la identificación de comportamientos anómalos. La aplicación del escepticismo y el juicio profesionales mejoran cuando el auditor tiene una adecuada comprensión de la entidad y de su entorno.

Limitaciones. Si bien los beneficios son claros, también hay limitaciones que los auditores deben tener en cuenta al usar estas herramientas y técnicas. Por ejemplo:

a) Los auditores deben tener una **comprensión** clara de los datos que están analizando, en particular su **pertinencia** para los fines de la auditoría. El análisis de datos que no son relevantes para la auditoría, que no están bien controlados, que no son confiables o cuya fuente (interna o externa) no se entiende bien, podría tener consecuencias negativas para la calidad de la auditoría.

b) Debido a la necesidad de que el auditor ejerza juicios profesionales en relación con la contabilidad y la auditoría, así como a cuestiones relacionadas con la completitud y validez de los datos, poder realizar pruebas al 100% de una población **no implica que el auditor sea capaz de proporcionar algo más que una opinión de seguridad razonable** o que el significado de "seguridad razonable" cambie.

c) En los estados financieros de la mayoría de las entidades, hay cantidades y revelaciones significativas que se basan estimaciones contables o que contienen información cualitativa. En estos casos es necesario aplicar el juicio profesional para evaluar la razonabilidad del valor estimado por la entidad y la información revelada de esos elementos. Si bien actualmente la tecnología de análisis de datos puede

proporcionar información valiosa para que el auditor la considere, su uso en una auditoría de estados financieros **no reemplaza la necesidad de aplicar el juicio y escepticismo profesionales**.

d) El uso eficaz de la tecnología puede ayudar al auditor a obtener evidencia de auditoría suficiente y adecuada. Sin embargo, se debe tener precaución con respecto al potencial "**exceso de confianza**" del auditor en la tecnología por parte de aquellos auditores que careciendo de un conocimiento claro de sus usos y limitaciones creen falsamente que los resultados son infalibles porque un programa de software los produjo. (Véase el apartado 10 de la GPF-OCEX 1503).

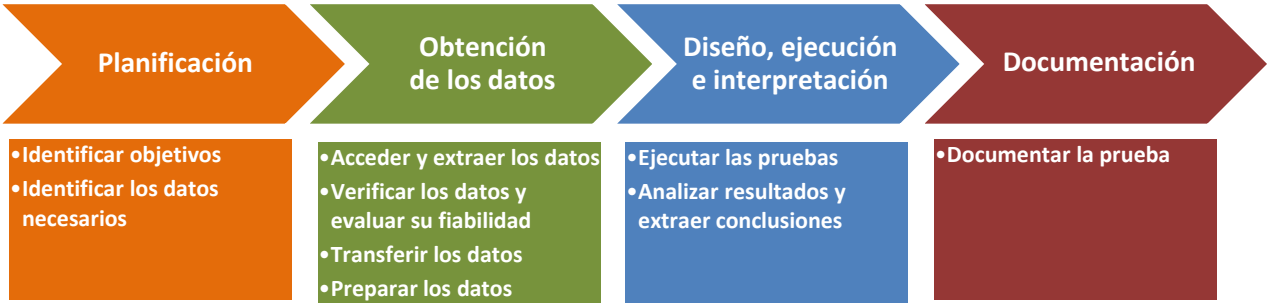
e) Necesidad de **formación específica** del personal auditor.

f) No siempre resulta sencillo **acceder a la información** debidamente actualizada y en un formato apropiado para tratarla de manera eficiente, además, puede haber reticencias por parte de los auditados que no estén demasiado dispuestos a compartir estos datos por miedo a perder su integridad o confidencialidad.

Sintetizando:

7. Etapas para la realización de una prueba de datos

La realización de una prueba de datos comprende las etapas siguientes:



En la práctica estas etapas pueden suceder de forma simultánea o en un orden distinto al anterior. También hay que considerar que estas etapas pueden ejecutarse de forma iterativa, es decir, puede haber información nueva o adicional que obligue a hacer cambios en el diseño inicial de las pruebas de datos planificadas.

II LA PLANIFICACIÓN DE UNA PRUEBA DE DATOS

8. ¿Cómo afecta a las actividades de planificación el posible uso de HTA/ADA en una auditoría? [14]

El auditor podrá considerar la posibilidad de utilizar HTA/ADA cuando lleve a cabo procedimientos de auditoría, tanto procedimientos de valoración de riesgos como procedimientos de auditoría posteriores. El auditor debe tener en cuenta que la utilización de HTA/ADA requiere que en la fase de planificación se consideren debidamente las implicaciones para la auditoría.

[14] El contenido del apartados 9 es una traducción no oficial del documento NON-AUTHORITATIVE SUPPORT MATERIAL: USING AUTOMATED TOOLS AND TECHNIQUES ON AUDIT PLANNING, de la IAASB publicado en diciembre de 2021, adaptado a las circunstancias de los OCEX.

Al establecer una estrategia general de auditoría y elaborar un plan de auditoría de conformidad con la NIA-ES-SP 1300, el auditor podrá considerar la posibilidad de utilizar HTA/ADA, cuando:

a) Realiza actividades preliminares a la auditoría.

b) Determina la naturaleza, el momento de realización y la extensión de los procedimientos de valoración del riesgo, con arreglo a la NIA-ES-SP 1315/GPF-OCEX 1315/NIA-ES 315R.

c) Determina la naturaleza, el momento de realización y la extensión de los procedimientos de auditoría posteriores previstos a nivel de afirmaciones en el marco de la NIA-ES-SP 1330.

d) Determina la naturaleza, calendario y la extensión de los recursos necesarios, incluido el uso del trabajo de un experto, para llevar a cabo el encargo.

e) Determina los demás procedimientos de auditoría que deben llevarse a cabo para que el trabajo cumpla con las NIA-ES-SP y GPF-OCEX.

f) Planifica la naturaleza, el momento de realización y la extensión de la dirección y supervisión de los miembros del equipo de auditoría y la revisión de su trabajo.

La utilización de HTA durante la auditoría y la forma en que esto puede afectar a las actividades de planificación son cuestiones que deben ser juzgadas por el auditor dadas las circunstancias de cada auditoría, pero normalmente afectará a: las actividades preliminares; la determinación de la naturaleza y la extensión de los procedimientos, incluidos los procedimientos de valoración de riesgos y procedimientos de auditoría posteriores; la determinación del momento de realización de los procedimientos de auditoría, y la consideración de la competencia y las capacidades de los recursos humanos necesarios para llevar a cabo el encargo.

Determinación de la naturaleza y el alcance de los procedimientos

Cuando existe la oportunidad de utilizar HTA/ADA en una auditoría, es útil considerar **cómo puede utilizarse la HTA/ADA para llevar a cabo un procedimiento de auditoría, qué objetivos de auditoría se propone abordar y qué HTA/ADA está a disposición del auditor**.

Inicialmente se pueden tener en cuenta los procedimientos aplicados en auditorías similares (por ejemplo, en otra auditoría se utilizó una determinada prueba de datos para un procedimiento en una situación similar) o los conocimientos adquiridos durante las auditorías del período anterior (por ejemplo, un determinado procedimiento manual que es repetitivo o ineficiente y podría beneficiarse de la automatización; o un procedimiento realizado con HTA/ADA el año anterior puede ampliarse para verificar controles adicionales o realizar otras pruebas añadidas).

La idoneidad del HTA/ADA puede basarse en la naturaleza de la actividad y las transacciones del auditado (por ejemplo, **puede ser particularmente apropiado cuando hay un gran volumen de transacciones similares que están sujetas a procesos y controles automatizados, como en los entornos de administración electrónica avanzada**), el software y la tecnología utilizados por el ente y la **facilidad de obtener los datos**.

Determinación del calendario de los procedimientos

Cuando se utiliza HTA/ADA en la realización de procedimientos de auditoría, su calendario puede verse afectado por las siguientes cuestiones:

- La **obtención y preparación de los datos** es un requisito previo para la realización de una prueba de datos.

  Por consiguiente, el plan de auditoría incluirá hitos clave para extraer y, cuando proceda, organizar o «limpiar» datos para su uso con ADA, dando tiempo suficiente para llevar a cabo dichas actividades. Para algunas auditorías, puede haber momentos clave en los que se necesite obtener datos, antes o después de que se completen determinadas rutinas contables.

- Evaluar si la información es suficientemente **fiable** para los fines del auditor[15], incluso si es exacta y completa, puede requerir más tiempo cuando haya una mayor variedad y volumen de datos para evaluar.

[15] Párrafo 9 de NIA-ES-SP 1500 y GPF-OCEX 1503.

- Dar tiempo suficiente para analizar el resultado del procedimiento, por ejemplo:
  - Que el auditor complete su conocimiento de la entidad y para el diseño de la prueba (por ejemplo, depurando los parámetros o la población); o
  - Que el auditor investigue las excepciones identificadas en el procedimiento de auditoría.

    Es muy importante considerar esta tarea cuando se realiza la planificación porque, en determinadas ocasiones, puede conllevar trabajos adicionales. Un ejemplo muy habitual es que, a partir del análisis de anomalías, se identifiquen nuevos flujos y tipos de transacción que requieran la realización de pruebas adicionales y, además, la obtención de nuevos datos necesarios para llevarlas a cabo.

¿Quién puede participar en actividades de planificación cuando se va a utilizar HTA/ADA en la realización de procedimientos de auditoría?

Cuando existe la posibilidad de utilizar HTA/ADA en una auditoría, puede ser útil incluir en el proceso de planificación a especialistas en HTA/ADA o a miembros del equipo de auditoría con competencias especializadas a fin de identificar oportunidades específicas para utilizar HTA/ADA y diseñar procedimientos de auditoría adecuados.

La participación de estas personas puede ayudar a:

- Evaluar si el ADA es apropiado y viable para su uso en las circunstancias particulares de la auditoría y si es probable que el ADA sea eficaz.
- Conocer y determinar el objetivo y alcance de los procedimientos que deben llevarse a cabo utilizando ADA.
- Conocer qué datos serán necesarios para llevar a cabo los procedimientos utilizando ADA.
- Comprender los resultados del ADA y qué análisis y evaluación deben llevarse a cabo para concluir sobre los resultados del procedimiento y las evidencias de auditoría obtenidas.
- Establecer la naturaleza, el calendario y la extensión de la dirección y supervisión de los miembros del equipo, así como la revisión de su trabajo, incluida la consideración de las aptitudes y los conocimientos especializados de quienes desempeñan funciones de dirección, supervisión y revisión.

Cuando aún no se esté considerando la posibilidad de utilizar ADA en una auditoría, la inclusión en la reunión de planificación de la auditoría o en el proceso de planificación de un especialista que se centre en el ADA puede proporcionar perspectivas alternativas al enfoque de auditoría.

9. Planificación y diseño de las pruebas de datos (ADA)

Las pruebas de datos deben planificarse con todo detalle. Es importante obtener, y entender, información detallada sobre, entre otras cosas, el sistema que alberga los datos (ficheros, gestor de base de datos, etc.), sobre las relaciones entre tablas y archivos, el modelo de datos, los controles totales, el tamaño, el formato de datos y la documentación del sistema, con carácter previo.

Al diseñar las pruebas de datos, el auditor debe tener claros los objetivos que desea lograr y la forma de alcanzarlos, ya que la información que se seleccione y solicite dependerá de los objetivos definidos y del alcance.

Cuanto más compleja sea la prueba, mayor será la necesidad de realizar una cuidadosa y detallada planificación. En estos casos se recomienda que el equipo de auditoría solicite la colaboración del equipo de especialistas del OCEX.

A la inversa, pruebas sencillas y rutinarias requerirán un menor trabajo en esta fase, pudiendo bastar en muchos casos la documentación final del trabajo.

La posible utilización de ADA durante la auditoría afecta a las actividades de planificación, incluidas las actividades preliminares, la determinación de la naturaleza y la extensión de los procedimientos, incluidos los procedimientos de valoración de riesgos y otros procedimientos de auditoría, la determinación del calendario de los procedimientos y la consideración de la competencia y las capacidades de los recursos humanos necesarios para llevar a cabo el encargo.

Enmarcadas en la etapa de planificación y diseño de las pruebas, **el auditor deberá llevar a cabo una serie de tareas, no necesariamente en el orden en el que se señalan seguidamente**:

a) Definir los objetivos concretos de la prueba

La realización de pruebas de datos es útil para llevar a cabo diferentes tipos de procedimientos de auditoría, por ejemplo: pruebas de controles, procedimientos analíticos o bien la realización de pruebas sustantivas de detalle para obtener evidencia sobre la completitud, exactitud y validez de la información generada por el sistema de información.

La definición de los objetivos de la prueba no está condicionada por el mecanismo de obtención de la información necesaria para realizarla, sino que será al revés: en función de los objetivos de la prueba y con ello, de la información que sea necesario analizar, se seleccionará el procedimiento de obtención de los datos que resulte más conveniente, en términos de fiabilidad de la evidencia de auditoría y de eficiencia en la realización del trabajo.

Los objetivos pueden ser los siguientes:

- Realizar pruebas de controles.

  Por ejemplo:

  - *Comprobar que todos los pedidos de compras están **autorizados** sólo por las personas que lo pueden autorizar.*
  - *Verificar la existencia de una adecuada **segregación de funciones** incompatibles al auditar el proceso de compras de una entidad. Se cruzarán las tablas que contienen la información de los usuarios autorizados a realizar ciertas transacciones, para detectar los usuarios que están autorizados en varias tareas incompatibles.*

- Procedimientos sustantivos: Obtener evidencia sobre la completitud, exactitud y validez de la información generada por el sistema de información.

  Por ejemplo:

  - *Comprobar que las facturas de compras coinciden en cantidades con el pedido y el albarán o entrada en almacén.*
  - *Verificar el correcto cálculo de la nómina mensual a partir de los datos fuente (maestro de personal).*

- Realizar procedimientos analíticos sustantivos.

  Por ejemplo, realizar un análisis Benford de todos los pagos bancarios del ejercicio.

b) Competencias y capacidades del equipo

De acuerdo con la GPF-OCEX 1220 (párrafo 20) **el auditor jefe debe asegurarse de que tanto el equipo de auditoría como, en su caso, los expertos externos cuenten, en su conjunto, con la competencia y capacidad adecuada**.

Cuando se utiliza ADA, esta determinación puede incluir la capacidad del personal para utilizar herramientas tecnológicas o contar con expertos apropiados, especialmente cuando la tecnología es más compleja, para acceder a los datos y evaluar su exactitud y completitud. Se considerará la complejidad del ADA que se utilizará para llevar a cabo el procedimiento y la dificultad de obtener los datos necesarios.

Las políticas o procedimientos del OCEX pueden requerir que el equipo de auditoría cuente con recursos especializados (como un grupo de auditoría informática interna) cuando se espera que se encuentren circunstancias específicas en la auditoría.

c) Qué datos están disponibles y dónde se encuentran

Después de establecer un objetivo claro para el uso de los datos es importante determinar qué datos son necesarios para alcanzar el objetivo de las pruebas, si están realmente disponibles, dónde se encuentran y si pueden extraerse de forma que se puedan utilizar de forma oportuna en el tiempo.

Esta comprensión más profunda de los datos del auditado puede aumentar la eficiencia y eficacia de la auditoría, por ejemplo:

- Posibilitando la selección de las fuentes de datos primarias, como el sistema ERP subyacente, en lugar de los informes generados por los entes auditados; y

- Analizando un conjunto de datos que se utilicen en múltiples procedimientos a lo largo de una auditoría y que pueda reutilizarse de manera eficiente en los años siguientes.

Los auditores considerarán:

- Si los datos necesarios para alcanzar el objetivo **están disponibles y son accesibles** por el auditor.

  Esto incluye determinar si los datos proceden de una fuente de información interna o externa, ya que esto puede afectar a la disponibilidad y oportunidad.

  El auditor debe considerar la disponibilidad de los datos en el momento en que está prevista la realización de las pruebas según el plan de auditoría. Por ejemplo, debe conocer la fecha límite para contabilizar todas las transacciones en el diario/mayor al final del ejercicio ya que, si los datos se recogen antes de esta fecha, existe el riesgo de que estos sean incompletos o inexactos.

  También, se debe considerar que hay datos que pueden no estar disponibles en un determinado momento (porque se actualizan posteriormente, porque se archivan y es más difícil obtenerlos, etc.). Si ese es el caso, el auditor puede solicitar a la entidad auditada la realización de una copia de dicha información o el que se realice una descarga previa a la modificación de esta.

- El **volumen** de los datos que se espera extraer y transferir.
- La **naturaleza** de los datos (por ejemplo, si se trata de datos financieros, no financieros, maestros, datos de configuración del sistema o informes) y si existen requisitos específicos de **confidencialidad y privacidad** que deben considerarse en su obtención y almacenamiento.
- Cuando los datos procedan de una fuente interna, **identificar el sistema o sistemas específicos de los que se obtendrán los datos** y conocerlo con suficiente detalle para determinar si existen limitaciones o problemas inherentes al sistema. Esto puede implicar el conocimiento de:
  - La complejidad del sistema, que puede afectar a la comprensión de la información a obtener.
  - El nivel de personalización del sistema auditado: si el ente auditado utiliza un ERP, el auditor debe obtener información de su grado de personalización (p.e. en un sistema SAP esto equivaldría a las denominadas transacciones Z*). Esto es necesario ya que, de no tenerlo en cuenta, el auditor podría seleccionar para su análisis datos erróneos o incompletos o diseñar pruebas que no se ajustan a la lógica de los procesos de gestión soportados por el ERP).
  - Conectividad y dependencia de otros sistemas y el nivel de automatización existente: esto implica identificar y analizar las interfaces existentes en el sistema auditado (por ejemplo, la existencia de transferencias manuales de información entre sistemas o de interfaces automatizadas y la tecnología con que están implementadas (transferencia de ficheros automatizada, uso de servicios web, etc.).
  - Controles sobre la preparación y mantenimiento de datos.

d) Conversaciones preliminares con la dirección de la entidad

Con objeto de que los responsables aprueben sin problemas la entrega de datos al auditor, es necesario explicarles claramente qué uso se dará a los datos y que se manejarán con las condiciones de seguridad adecuadas. Esto es especialmente importante la primera vez que se tiene acceso las bases de datos completas o acceso a la aplicación de gestión para la obtención de listados de forma autónoma por el auditor. Si el auditor hace un uso adecuado del acceso que se le otorgue, en posteriores auditorías esta dificultad habrá desaparecido con toda probabilidad.

Cuando se vaya a realizar una prueba de datos, las actividades preliminares pueden incluir **conversaciones con la dirección de la entidad** sobre cuestiones tales como:

- Los **objetivos generales de las pruebas a realizar y las necesidades de colaboración** por parte de la entidad auditada para llevar a cabo esta parte del trabajo. Esto incluirá la previsión de reuniones a mantener y el personal implicado, así como el acceso los datos, sistemas y aplicaciones que se requieran.
- **La calidad y fiabilidad de los datos**, incluida la forma en que la entidad auditada mantiene su integridad, los procesos y los controles existentes, y quién tiene acceso a los datos.
- **Si es posible utilizar datos anonimizados**, siempre que con ellos se pueda lograr los objetivos de las pruebas planificadas.

- **Planificación prevista para la realización de la prueba,** planteando fecha tentativa en la que el auditor necesitará disponer de los datos.
- **Dónde se almacenarán los datos** de la entidad antes, durante y después de la ejecución de los procedimientos de auditoría.

Cuando sea pertinente, las conversaciones también podrán incluir cualquier aspecto legal o reglamentario relacionado con los datos de la entidad, incluyendo la salida de los datos del ámbito nacional (consideraciones a realizar en entornos *cloud*).

En determinadas situaciones, los acuerdos alcanzados en la reunión de este apartado y en la del siguiente sobre acceso a la información, plazos, etc. puede ser conveniente reflejarlos en el **DIA** (ver apartado 10).

e) Identificar al propietario de los datos o responsable funcional y al responsable técnico de la aplicación auditada

El auditor mantendrá una reunión con el responsable funcional (propietario de los datos) y con el responsable técnico de la aplicación del departamento de sistemas con el objetivo de planificar la realización de la prueba de datos, analizar su viabilidad y acordar los procedimientos de obtención de la información, de forma que se pueda identificar y resolver cualquier duda, cuestión o dificultad en relación con esta.

Para ello, en esta reunión se deben tratar, entre otros, los siguientes aspectos:

- Explicar de forma general las pruebas que se van a realizar, evaluando de forma conjunta entre el auditor y los responsables la viabilidad y eficacia de la prueba planteada.
- Identificar los datos que potencialmente se necesitarán y el procedimiento para su obtención que, en cualquier caso, debe permitir un doble objetivo:
  - Garantizar la integridad de la información ante cualquier fallo asociado a la intervención del auditor.
  - Asegurar la integridad de la información facilitada al auditor cuando es la entidad auditada la encargada de su extracción.
- Analizar la viabilidad de las diferentes alternativas de obtención de los datos (descarga de la información por parte de la entidad auditada, acceso directo por parte del auditor, formatos, etc.), con el fin de seleccionar la más adecuada. Más adelante se trata en profundidad este punto.
- Consensuar los plazos para la entrega de la información o la disponibilidad de los usuarios y accesos necesarios a los datos y sistemas involucrados en los casos en los que sea necesario.

Esta reunión es muy importante para el buen desarrollo de las pruebas.

f) Conocer y analizar el proceso de gestión auditado.

El auditor debe obtener una descripción general tanto del sistema TI como específicamente del proceso de gestión auditado, identificando el flujo de información a lo largo del proceso, la interacción con los repositorios de datos subyacentes (bases de datos, ficheros, etc.), los controles generales y de aplicación y la disponibilidad de los datos para los propósitos de auditoría. Todo este conocimiento forma parte del proceso normal de una auditoría y deberá adquirirse conjuntamente entre el personal del equipo de auditoría y el experto en ADA del OCEX integrado en el equipo.

Conviene hacer una breve descripción del proceso de gestión para poner la prueba en su contexto. Para conocer el flujo de datos será conveniente disponer del flujograma del proceso de gestión que se está auditando.

Mediante este trabajo, los auditores también consiguen un mejor conocimiento del sistema de control interno que puede ser evaluado con pruebas específicas de auditoría usando ADA. La profundidad y extensión de este conocimiento dependerá de los objetivos y alcance de la fiscalización.

g) Comprender el modelo de datos de la aplicación auditada.

Entender los datos que se van a utilizar es más importante que los aspectos técnicos de las herramientas de análisis de datos. Es muy importante adquirir un conocimiento profundo de cómo están estructurados los datos y esto se consigue conociendo el **modelo de datos**[16] del sistema que se desea auditar y también el **flujo**

[16] Un modelo de datos consiste en una descripción de la estructura de una base de datos y de las relaciones existentes entre ellos.

de los datos a través del proceso de gestión auditado.

Sólo después de disponer de este conocimiento seremos capaces de pedir debidamente y obtener los datos necesarios, diseñar pruebas de auditoría eficaces, entender los resultados de la prueba y extraer conclusiones significativas.

En ciertos entornos, las bases de datos subyacentes pueden tener cientos, incluso miles de tablas, cada una con numerosos campos de datos con nombres ininteligibles para un no experto. Por lo tanto, es necesario que el equipo auditor cuente con especialistas capaces de obtener y entender el modelo de datos a auditar, para saber exactamente dónde (ficheros, base de datos (profundizando hasta el nivel de esquema, tablas y campos) se almacenan los datos de interés para los objetivos de la auditoría y cómo se interrelacionan entre las distintas tablas.

Para esto es necesario tener a reunión con el responsable de la aplicación del departamento TI que normalmente tendrá un conocimiento profundo de estas cuestiones.

Comprender los datos ayuda a saber lo que están mostrando los datos, y cómo interpretar los resultados obtenidos.

Se debe limitar lo posible el conocimiento del modelo de datos a aquellos datos importantes para los objetivos de auditoría para no perder tiempo innecesariamente.

En entidades en las que el conocimiento y documentación sobre el modelo de datos es limitado o inexistente, y no se ha realizado el trabajo anterior, determinar en una petición la información que el auditado debe facilitar es muy complicado. En estos casos, es muy común que conforme el auditor analiza la información facilitada se originen nuevas necesidades de información para poder llevar a cabo la prueba (tablas adicionales, incluir más campos en las tablas facilitadas, etc.).

Un problema que surge en la práctica, especialmente cuando se audita una aplicación comercial, es que el auditado no conoce el modelo de datos de su aplicación y es necesario insistir para obtenerlo del proveedor. Si surge este problema en una auditoría, debe revisarse el pliego de cláusulas administrativas y/o el pliego de cláusulas técnicas de la compra de la aplicación ya que de ordinario existirá una cláusula que establece que el adjudicatario está obligado a facilitar a la entidad contratante el modelo de datos de la aplicación adquirida.

Un problema adicional se presenta cuando se audita una aplicación cloud o SaaS, es decir, cuando los datos no están disponibles en los sistemas del auditado y hay que obtener las bases de datos de un tercero. En estos casos la obtención de los datos es más complicada, y si hay problemas también es aconsejable revisar los pliegos de contratación y el contrato de compra del servicio.

h) Selección de la información/datos clave a utilizar y el mecanismo de acceso/extracción de datos que se utilizará.

Una vez conocido el modelo de datos se determinarán las tablas y campos a utilizar; no se solicitarán campos irrelevantes. En los casos en los que el auditor vaya a acceder directamente a la información, también se respetará el principio anterior. En definitiva, sólo se solicitará/accederá a la información necesaria para la realización de las pruebas. El auditor evaluará si se está aplicando el principio de minimización (solicitar todos los datos necesarios, pero solo los necesarios), especialmente cuando se incluyan datos personales.

En línea con lo comentado en el punto anterior, en función del grado de conocimiento y documentación existente sobre el modelo de datos, la selección de la información clave a utilizar puede ser una tarea más o menos laboriosa y el grado de concreción puede variar.

Una parte importante del proceso de ejecución de una prueba de datos es documentar y explicar el proceso para **extraer, transferir, transformar** (incluida la carga en cualquier herramienta) y determinar la integridad de la información que debe utilizarse como prueba de auditoría.

Al considerar quién participará en esta etapa los auditores considerarán cuestiones tales como:

- ¿La extracción de datos será realizada por el auditado, el auditor o un experto?
- Cuando el ente auditado realice la extracción:
  - ¿Tiene el ente un conocimiento suficiente de los sistemas para poder extraer los datos necesarios para el auditor?
  - ¿La extracción puede ser realizada por el auditado de manera oportuna?

- ¿Qué procedimientos deberá realizar el auditor para determinar que el auditado no ha manipulado los datos durante la extracción o transferencia?

- Cuando la extracción sea realizada por el auditor:
  - ¿Qué herramientas se utilizarán para realizar la extracción?
  - ¿Cuáles son los procesos para determinar la fiabilidad de las herramientas utilizadas durante la extracción?
  - ¿Tiene el miembro del equipo de auditoría experiencia para poder utilizar las herramientas necesarias para extraer y preparar grandes volúmenes de datos?

  Si el equipo de auditoría accede a la información directamente a la base de datos se debe considerar la posibilidad de acceder a una copia fidedigna de la base de datos de producción (la realmente utilizada por la aplicación de gestión) para no afectar a la gestión diaria del proceso o adoptar otras precauciones con el mismo fin. En cualquier caso, debe asegurarse de que la extracción de datos no afecta al proceso de gestión real que se está auditando.

- Cuando se requiere un experto, ¿es interno o externo?

- ¿Los miembros del equipo de auditoría tienen un conocimiento suficiente del proceso de extracción, transferencia y transformación para poder identificar errores en el proceso?

Sobre los mecanismos de extracción de datos ver el apartado **III**

i) Diseñar la prueba antes de empezar a trabajar con los datos.

El diseño incluirá un diagrama de flujo estimativo de la prueba, para lo que se utilizarán los símbolos y metodología descritos más adelante.

j) Verificar la viabilidad técnica de la prueba.

Finalmente, hay que analizar si la prueba proyectada es factible. Este es un punto muy importante y hay que identificar de forma detallada la fuente de información (SAP HANA, Oracle, SQL Server, ficheros, etc.) y considerar las siguientes cuestiones:

- ¿Los datos se encuentran disponibles y pueden ser extraídos?
- ¿Se trata de un volumen muy grande de datos?
- ¿Tenemos capacidad para procesar toda la información requerida?
- De acuerdo con el diseño hecho, ¿consideramos que se pueden alcanzar los objetivos de la prueba?

Todo el proceso de planificación de la prueba se debe documentar de forma sucinta y clara. En el ***Anexo 6 Modelo para documentar la planificación de una prueba de datos*** se propone un modelo de papel de trabajo para esta etapa.

10. El documento de inicio de la auditoría (DIA) y la solicitud de la información

En determinados casos, como trabajos especiales, trabajos en los que se solicita por primera vez tablas o acceso directo a las bases de datos y/o a la aplicación de gestión o en aquellos que prevemos dificultades en la obtención de los datos, resultará conveniente incluir en el DIA una referencia explícita a esta materia y solicitar los accesos necesarios para la realización de la auditoría.

Ver ejemplo en ***Anexo 5 Ejemplo de contenido del DIA.***

Una vez enviado el DIA y realizada la selección de la información (base de datos, tablas y campos) que se desea procesar, se solicitarán los datos que se necesiten al responsable funcional o coordinador de la fiscalización en la entidad. Dicha petición inicial debe ser formal, a efectos de garantizar una clara delimitación de responsabilidades y posibilitar su documentación en los papeles de trabajo.

Ver ejemplo de petición en el ***Anexo 7 Modelo de petición de información.***

Para ver en mayor detalle cómo se puede solicitar y/o extraer la información, ver el apartado **III**.

11. Formato de los datos solicitados

A pesar de que las herramientas ADA permiten tratar varios formatos de archivo, algunos son más confiables que otros, por eso es importante seleccionar el formato más confiable disponible para solicitar y obtener los datos. Los principales formatos de archivo para la obtención de los datos origen son:

- Archivos de ancho fijo.
- Archivos delimitados.
- Archivos de Microsoft Excel/Access.
- Archivos XML
- Archivos de reporte (imagen de impresión).
- Archivos PDF.

A continuación, se detallan las principales características de cada uno de los formatos anteriores.

Archivos de ancho fijo

Un archivo de ancho fijo contiene datos sin definición de campos y cada campo tiene un ancho fijo. Para garantizar la uniformidad del ancho del campo, los valores se completan con espacios en blanco.

Archivos delimitados

A diferencia de los archivos de ancho fijo, los archivos delimitados tienen registros de ancho variable, ya que las diferentes longitudes de los campos no se completan con espacios en blanco. Los archivos delimitados separan los campos con delimitadores. Si bien se puede utilizar como delimitador cualquier carácter (";", "/", etc.), es recomendable que elijamos el que con menos probabilidad pueda aparecer como parte de un campo. Por ejemplo, "|".

Archivos de Microsoft Excel/Access

A pesar de que los archivos de Excel y Access se pueden tratar con la práctica totalidad de herramientas de análisis de datos, no son los formatos más recomendables. Esto es debido a que los datos originales deben ser convertidos desde el servidor a Excel y dicho proceso de conversión puede dañar los datos (por ejemplo, por pérdida de espacios en blanco o ceros a la izquierda). Además, la limitación de tamaño de Excel puede dar lugar a que se generen varios archivos de Excel para un conjunto de datos. Esto hace más costoso el proceso de importación y, a su vez, aumenta la probabilidad de que se produzcan errores.

Archivos XML

Un archivo XML es un archivo de texto con etiquetas. Según el esquema que siga (XSD) se puede abrir con el programa Excel con un resultado óptimo o quizá requiera tratarlo automáticamente con un programa especial que decodifique las etiquetas,

Archivos de reporte

Un archivo de reporte es una copia digital de un reporte impreso. Contiene saltos de página con la información de encabezado repetida en cada página. El uso de archivos de reporte únicamente es aconsejable cuando los otros tipos de archivos no estén disponibles o cuando sea necesario auditar o analizar la precisión del propio reporte. La estructura de los archivos de reporte puede variar mucho y la importación de este tipo de ficheros a la herramienta de análisis de datos suele ser compleja.

Archivos PDF

A pesar de que los archivos PDF se utilizan con mucha frecuencia (fundamentalmente para informes de seguimiento, gestión de incidencias, etc.), no son el formato más aconsejable y deben utilizarse únicamente cuando no estén disponibles los formatos alternativos, como archivos delimitados o de ancho fijo.

Si el auditor accede directamente a la base de datos no es necesario definir el formato de los datos a extraer. En otro caso, debemos expresar los formatos de los datos solicitados (ver apartado siguiente).

III ACCESO Y EXTRACCIÓN DE LOS DATOS

Como ya se ha expuesto, una de las etapas de la planificación de una prueba de datos consiste en la solicitud y obtención de la información que será posteriormente analizada mediante una herramienta ADA.

El objetivo de este apartado es analizar las diferentes formas de obtención de la información necesaria para la realización de una prueba de datos, con el fin **de facilitar al auditor la selección del método más adecuado en términos de eficacia y eficiencia**.

12. Criterios generales para obtener la información necesaria para realizar una prueba de datos

El auditor deberá atender siempre, con independencia del mecanismo de obtención de información seleccionado, las siguientes directrices para la obtención de la información necesaria para llevar a cabo una prueba de datos:

- La obtención de información debe seguir **procedimientos estándar** para **garantizar la protección de los sistemas de información del auditado, así como la integridad de los datos recogidos y su fiabilidad**. Esto implica que **en ningún caso el auditor deberá tener acceso a los sistemas del auditado con permisos de escritura/modificación de los datos**.

  Esto implica en lo siguiente:

  - Si el acceso se realiza a nivel de base de datos, el usuario de conexión dispondrá únicamente de privilegios de lectura de los datos.
  - Si el acceso consiste en un usuario en la aplicación de gestión, los permisos asociados se limitarán igualmente a consulta y extracción de listados, sin que en ningún caso el auditor disponga de los privilegios necesarios para realizar tareas de gestión (ejemplos: crear/eliminar registros o expedientes, modificar expedientes y trámites en curso, realizar apuntes contables, etc.).
- El auditor/OCEX debe prestar atención especial a la **seguridad de la información** tratada.

  En el trabajo con grandes bases de datos de organismos públicos, que incluyen datos económicos y datos personales, los auditores deben tener especial cuidado con las cuestiones relacionadas con la seguridad de la información, especialmente con su integridad, confidencialidad y privacidad, tanto en la transmisión como en su almacenamiento.

  Criterios de mínimos de seguridad son los siguientes:

  - La transmisión debe realizarse por un medio que permita su cifrado.
  - El tratamiento y almacenamiento debe realizarse preferentemente en los sistemas centrales del OCEX, evitando utilizar para ello dispositivos portátiles (ordenadores portátiles, USBs, etc.). En el caso de que el uso de dispositivos portátiles sea necesario, será obligatorio que estos incorporen mecanismos de cifrado y, en todo caso, dichos medios se utilizarán únicamente con carácter temporal. La ubicación definitiva debe realizarse en los sistemas centrales del OCEX.
  - Los sistemas centrales del OCEX deberán contar con las medidas de seguridad necesarias para permitir la seguridad de la información almacenada (cumplimiento del ENS).
- Se deben considerar los **aspectos legales** relacionados con la seguridad y con la protección de datos personales.
- La **solicitud** de información **debe indicar exactamente qué datos se necesitan** (tablas y campos) evitando solicitar información innecesaria que no vayamos a utilizar posteriormente en los análisis. Esta directriz será igualmente aplicable si el auditor es el que realiza directamente las extracciones de datos, esto es, no extraerá información que no resulte necesaria para llevar a cabo la prueba.
- La información deberá ser obtenida directamente de las tablas originales de la base de datos (normalmente sólo con el filtro correspondiente al ejercicio fiscalizado), sin que se realicen consultas o se establezcan criterios de filtrado adicionales.
- En los casos en que la información facilitada haya sido extraída por personal de la entidad auditada utilizando filtros o cruces entre varias tablas, se solicitará el detalle de dichos tratamientos (programas, consultas *(queries)*, impresiones de pantalla de las condiciones de extracción, etc.) y se verificará que no se ha filtrado información que podría ser relevante para el análisis.

Cuando la explicación facilitada por los técnicos sobre la extracción no sea satisfactoria o comprensible, se consultará a los expertos en ADA del OCEX.

Si es el auditor el encargado de realizar las extracciones de información y aplica tratamientos previos para la extracción de datos, estos deberán quedar reflejados y debidamente explicados en la documentación de la prueba.

- Con independencia del mecanismo de extracción utilizado, el auditor deberá realizar pruebas que le permitan obtener seguridad sobre la integridad y fiabilidad de la información a analizar (ver apartado 13).
- El procedimiento de acceso directo a las bases de datos en las que reside la información a analizar únicamente deberá realizarse con la colaboración de expertos del OCEX.

13. Procedimientos de obtención de la información para realizar una prueba de datos

En esta sección se analizan diferentes alternativas para la obtención de la información para llevar a cabo pruebas de datos que se deben considerar en cada uno de los trabajos de fiscalización, incluyendo ventajas e inconvenientes de cada una de ellas.

Las opciones varían en función de:

- Quién obtenga la información: auditor o auditado.
- Origen de los datos.
- Mecanismos y herramientas de extracción.

a) Extracción de la información por parte del auditor o la entidad auditada

La información necesaria para realizar una prueba de datos la puede extraer de los sistemas de información de la entidad tanto el personal del ente auditado como directamente el auditor.

De manera general, en peticiones de información muy concretas y acotadas, se puede optar porque sea la propia entidad quien facilite la información. En ese caso, el auditor deberá realizar controles adicionales que permitan verificar la integridad de la evidencia obtenida (además de los destinados a evaluar su fiabilidad). Dependiendo del mecanismo utilizado para la extracción, dichas pruebas variarán. Por ejemplo, en el caso de descarga de tablas, solicitar datos de control como número de registros descargados, totales de campos numéricos, rangos de fecha, etc. También puede ser conveniente realizar pruebas de muestreo.

Sin embargo, la extracción por parte del auditor de la información necesaria para realizar la prueba de datos es conveniente cuando:

- El auditor considera que la extracción directa por su parte es la única forma de garantizar la integridad de la información a analizar para obtener evidencia de auditoría suficiente y adecuada.
- El esfuerzo asociado a la extracción de la información no puede ser asumido por la entidad o, en su caso, los plazos necesarios para la obtención de dicha información impactan negativamente en la auditoría y la realización de esta tarea por parte del auditor agiliza el proceso.
- El conocimiento del modelo de datos es limitado o inexistente, de forma que inevitablemente el diseño de la prueba no se puede llevar a cabo sin que el auditor examine la estructura y contenido de los datos.

b) Origen de los datos

La información obtenida debe proporcionar, en cualquier caso y con independencia de su origen, una evidencia de auditoría fiable y para eso es necesario que tanto la fuente de los datos sea fiable y completa como que el método para extraerlos garantice esa fiabilidad y completitud.

Partiendo de la premisa anterior, en la práctica puede haber varias alternativas en cuanto al origen de los datos:

i. De entornos de producción

Por defecto, consideraremos siempre la obtención de la evidencia a partir de los datos existentes en el entorno de producción, que contiene directamente los datos que se generan como consecuencia de la operativa de la entidad.

No obstante, cuando se obtienen datos directamente del entorno de producción, especialmente si es el auditor quien realiza las extracciones, se debe tener en cuenta las siguientes consideraciones:

- Es imprescindible **garantizar que los datos no pueden ser modificados** como consecuencia de la extracción.

  Para ello, será condición indispensable si se quiere utilizar este entorno que el nivel de acceso que la entidad facilite al auditor únicamente permita la lectura y extracción de información, nunca su alteración o borrado. Si lo anterior no se puede garantizar, el auditor **no** accederá a dicho entorno de manera independiente.

- La extracción de los datos **no debe afectar negativamente a la operativa** de la entidad.

  Las operaciones de extracción de datos (bien sea descarga de tablas de bases de datos, ejecución de informes predefinidos, listados, etc.) conllevan un nivel de procesamiento que consume recursos de los sistemas de información. En ocasiones, debido a diferentes motivos (volumen de información, complejidad de las consultas necesarias para extraerla, diseños inadecuados de la base de datos o de los informes, etc.) las operaciones de extracción de datos pueden consumir un volumen de recursos demasiado alto, penalizando el rendimiento del sistema o aplicación hasta el punto de que podrían bloquearlo y dejarlo inoperativo para el personal de la propia entidad.

  Por ello, si en la planificación del trabajo, concretamente en la reunión del auditor con los responsables funcional y técnico de la aplicación, se detecta este riesgo, se deberá buscar otras alternativas como, por ejemplo, pactar ventanas temporales para la extracción de la información (periodos en los que la carga del sistema sea baja) o bien extraer la información de otros orígenes.

ii. Entornos de preproducción, formación, entornos de respaldo, etc.

Se utilizará si las circunstancias desaconsejan la obtención directa del entorno de producción, para evitar bajadas de rendimiento del sistema, por ejemplo.

Hay entidades que cuentan con entornos independientes al de producción en los que se dispone de los mismos datos que en el entorno productivo y que se utilizan con fines concretos, como puede ser la formación a usuarios, la realización de determinadas pruebas (como, por ejemplo, pruebas de carga) o bien entornos que contienen copia de los datos de producción para garantizar la alta disponibilidad de la información en caso de incidente.

iii. Datawarehouse o sistemas de bussiness intelligence.

Hay entidades que cuentan con repositorios de datos independientes a las bases de datos que dan soporte al entorno transaccional, que se nutren de estas últimas y que se utilizan para otros propósitos, como, por ejemplo, el reporting. Como ejemplo, se tienen los almacenes de datos o las bases de datos sobre las que trabajan las aplicaciones de bussiness intelligence.

Estos datos, aunque también forman parte del entorno de producción, suelen tener requisitos de disponibilidad menos exigentes que las bases de datos que soportan la operativa transaccional y una disminución temporal del rendimiento de estos sistemas puede ser tolerada sin afectar a la gestión habitual de la entidad. Es por ello, por lo que estos entornos pueden ser considerados a la hora de extraer la información.

El auditor junto con la entidad analizará la mejor opción a utilizar como origen en el proceso de extracción de datos, siempre que se pueda garantizar la integridad de la información obtenida. Si se plantea utilizar un entorno distinto al de producción, el auditor debe obtener información sobre las siguientes cuestiones:

- El mecanismo utilizado para cargar datos del entorno

  Extracción de determinadas tablas de producción y volcado, copia completa de base de datos, clonado de la máquina virtual, etc.

- Tratamientos o lógica adicional aplicada en el proceso de carga de datos del entorno.

  Si la información de un entorno de preproducción, por ejemplo, no se genera directamente mediante copia completa de base de datos o de máquina virtual, sino que se utilizan tratamientos complementarios en la exportación/importación de datos, el auditor deberá obtener conocimiento sobre dichos tratamientos para determinar si estos modifican los datos originales de forma que los hace inservibles para el propósito de la prueba.

No siempre el hecho de que se apliquen tratamientos que alteran los datos originales los hace inservibles para la realización de las pruebas de datos. Por ejemplo, suele ser común que, para garantizar la confidencialidad, la entidad aplique mecanismos de ofuscación o disociación de datos.

En estos casos, el auditor debe analizar si la modificación de los datos afecta a la prueba. Por ejemplo, en una prueba sobre antigüedad de la deuda, la modificación de la información existente en un entorno de preproducción sobre la persona de contacto del proveedor (nombre y apellidos, teléfono, etc.) no afecta al objetivo de la prueba, por lo que dicho origen de datos sí podría ser utilizado. Por el contrario, en una prueba de nómina, si el dato que identifica a la persona perceptora se enmascara, no podremos realizar pruebas cuyo objetivo sea identificar perceptores que no están trabajando en la entidad.

- Vigencia de la información

  Para ello, se deberá conocer la frecuencia de actualización de los datos del entorno que se pretende utilizar. El periodo de actualización de la información debe ser coherente con el ámbito temporal que comprende la fiscalización.

- Integridad de la información existente en el entorno tras su carga

  Además de que el proceso de carga de datos desde el entorno real al entorno secundario debe permitir asegurar la integridad de los datos, el auditor debe garantizar que tras su carga dicha información no es modificada. Para ello, necesitará conocer el uso que se le da a ese entorno y, en su caso, acordar con la entidad una ventana en la que no se podrán realizar modificaciones sobre la información existente.

c) Mecanismos y herramientas de extracción de datos

Existen diferentes alternativas a la hora de extraer los datos almacenados en bases de datos que serán objeto de análisis.

Dependiendo de la entidad, los sistemas de información que utilice (aplicaciones, gestores de bases de datos, etc.) el auditor junto con el personal de la entidad deberá analizar las alternativas existentes y seleccionar la que resulte más apropiada en cada caso.

A continuación, se indican, a modo orientativo, los mecanismos más comunes de extracción de información almacenada en bases de datos.

i. Descarga directa de las tablas de bases de datos en las que se encuentra la información.

Para ello, la sentencia SQL para la extracción de datos sería de la siguiente forma:

```
select * from <nombre_tabla>
```

La extracción de datos realizando una consulta directa a las bases de datos es uno de los mecanismos que proporcionan una evidencia más fiable, en la medida, en que permite partir de los datos “en crudo”, sin que se realicen tratamientos que podrían alterar (bien por error o bien porque el auditor no lo tenga en cuenta en el diseño de la prueba) la información sobre la que se realiza la prueba de datos, lo que conllevaría la obtención de resultados erróneos.

ii. Descarga de las tablas de bases de datos aplicando tratamientos previos.

Para ello, la sentencia SQL para la extracción de datos sería de la siguiente forma:

```
select * from <nombre_tabla> WHERE <condiciones>
```

Siempre que se utilice este mecanismo de extracción, la documentación de la prueba debe incluir la consulta utilizada para la obtención de la información. Si es el auditor el que realiza la consulta, los papeles de trabajo incluirán el detalle de la consulta utilizada, explicando claramente la lógica aplicada y el motivo por el que se aplica (por ejemplo, “se aplica filtrado por fechas, utilizando el campo XXXX, para obtener únicamente los documentos contables registrados en la contabilidad durante el año fiscalizado” o “se aplica filtrado por tipo de expediente, utilizando para ello el campo “xxxxx”, para seleccionar únicamente los expedientes correspondientes al tributo analizado”, etc.).

Cuando es el personal de la entidad auditada el encargado de realizar la extracción, con carácter previo, el auditor indicará explícitamente los mecanismos de filtrado a aplicar y comprobará que únicamente dichos criterios han sido aplicados en la consulta realizada por la entidad. Tanto los datos como el diseño de la consulta se archivarán como papeles de trabajo.

iii. Uso de informes y listados predefinidos de la aplicación.

Estos mecanismos, aunque suelen proporcionar agilidad en cuanto a la obtención de datos, conllevan el inconveniente de que el auditor debe plantear pruebas adicionales para verificar la integridad de la información facilitada y cuya realización, en sí misma, puede suponer una prueba de datos adicional.

Por ejemplo, si el auditor debe comprobar la completitud y exactitud de un listado sobre "aging de facturas" obtenido directamente a partir de un informe de la aplicación, deberá:

- Analizar el código del programa que genera ese listado, tarea que puede ser compleja y no facilitar un nivel de fiabilidad suficiente.
- Realizar una prueba de muestreo que, dependiendo del número de deudores y de facturas, puede requerir que el tamaño de la muestra sea muy grande y con ello, el esfuerzo de realizarla sea elevado.
- Diseñar una prueba de datos a partir de la información origen que replique la obtención de dicho listado.

iv. Uso de informes y listados definidos ad-hoc.

En ocasiones, es posible que el auditado proponga la creación de un listado o informe que permita obtener los datos solicitados por el auditor.

En estos casos, análogamente a lo señalado en el punto anterior, el auditor deberá realizar pruebas adicionales que permitan garantizar la integridad de la información obtenida.

Además, de forma general, el uso de esta opción para la extracción de datos no es la más aconsejable, fundamentalmente por los siguientes motivos:

- Proporcionan una evidencia menos fiable que la obtención de los datos sin tratar.
- El coste que conlleva el crear un nuevo informe o listado (desarrollo, pruebas, pase a producción, etc.) suele ser elevado y el plazo temporal para llevarlo a cabo suele afectar negativamente a la realización del trabajo.

En definitiva, y a modo de resumen de este punto, concluiremos que, de manera general, en cuanto a los mecanismos de extracción de la información que se utilizará como base para la realización de pruebas de datos, **el auditor considerará como primera opción la obtención de los datos directamente desde la fuente y limitando al máximo los tratamientos de la información original (cruces, agrupaciones, etc.), salvo los filtros que sea indispensable aplicar para no extraer información innecesaria para la realización de la prueba**.

14. Mecanismos de extracción de la información mediante acceso directo a la base de datos

Para realizar la extracción directamente de las bases de datos existen diferentes alternativas, siendo las más utilizadas las siguientes:

a) Uso de un cliente SQL para el acceso y la extracción de datos

Los clientes SQL son utilidades que permiten la conexión y extracción de datos de una base de datos relacional. Existen multitud de clientes SQL tanto gratuitos como software propietario.

Cuando se opta por este mecanismo, los pasos a realizar serían los siguientes:

- Conexión a la base de datos utilizando el cliente SQL.
- Diseño de la consulta para descargar los datos.
- Selección del formato utilizado para la exportación de datos. Los distintos formatos posibles y la descripción de sus características se pueden consultar en el apartado 11 de esta guía.
- Importación de los datos extraídos en la herramienta de análisis (ACL).

El ***Anexo 8 Ejemplo de extracción de datos utilizando el cliente SQL Developer de Oracle*** proporciona información práctica para facilitar el uso de este procedimiento.

Si bien este mecanismo en general es adecuado, en determinados casos puede presentar ciertos problemas, fundamentalmente por las siguientes cuestiones:

- **Volumetría**. Si la cantidad de información a extraer es muy elevada, el proceso de exportación e importación pueden ser temporalmente muy costosos, e incluso, sobrepasar los recursos disponibles en la máquina donde reside la base de datos y, con ello, que el proceso de exportación resulte fallido.

  Además, el elevado tamaño de los ficheros también afecta negativamente a la transferencia de información, desde los sistemas del auditado hasta los equipos en los que el auditor realizará el análisis.

  Ante este problema, una solución puede ser "trocear" la información a descargar, utilizando para ello filtrados (por ejemplo, en una prueba de nómina, en lugar de realizar una única descarga con los registros de nómina de todos los perceptores durante todo el ejercicio fiscalizado, realizar doce descargas, correspondientes a las nóminas de cada mes).

- **Errores de formato**. En ciertas ocasiones, con independencia del formato elegido en el proceso de exportación, dicho proceso modifica ciertos datos sin que se pueda saber de antemano qué datos han sido modificados. Este error, identificado en la práctica, se da con mayor frecuencia en dos situaciones:

  - Cuando la tabla a descargar tiene campos de texto muy largos. Estos campos normalmente se incluyen para dejar un campo de texto abierto en el que incluir observaciones, comentarios, anotaciones, etc. durante la gestión. En estos casos, el proceso de exportación inserta un salto de línea que hace que, al cargar la información en la aplicación de análisis (ACL, Excel, etc.) la información correspondiente a un registro, que debe almacenarse en una única fila, se divida en dos.

  - En campos con formato fecha. En la práctica se ha observado que, sin motivo aparente, en determinadas situaciones los campos con formato de fecha son modificados en el proceso de extracción de datos.

b) Uso del programa ACL para la extracción de datos

Si el auditor utiliza el software ACL, este programa le permite acceder a una amplia variedad de tipos de archivo, bases de datos y orígenes de datos en la nube[17].

ACL cuenta con dos alternativas para el acceso a datos:

- Uso de la ventana Data Access para acceder a cualquier origen de datos ODBC. Esta utilidad incorpora, entre otros, conectores de datos nativos a orígenes de datos, como Oracle, Microsoft SQL Server, Salesforce, etc.
- En modo comando, lo que permite su uso en scripts, a través del comando ACCESSDATA.

En el ***Anexo 9 Ejemplo de conexión de ACL con una base de datos Oracle*** se incluye un ejemplo de uso que ilustra este procedimiento.

El realizar directamente la extracción y carga de datos mediante la utilidad ACL aporta, frente al uso de clientes SQL, las siguientes ventajas:

- Se reduce el tiempo asociado a la exportación e importación de los datos. El uso de los conectores integrados en la propia herramienta de análisis disminuye el tiempo y la complejidad de los procesos de extracción y carga.
- Disminuye los errores asociados a problemas de formato. El evitar la conversión de los datos almacenados en una tabla de base de datos a un fichero de texto y la posterior creación de la tabla en ACL, reduce los errores identificados en la práctica asociados al formato de los datos.
- El utilizar ACL como mecanismo de conexión también aporta un nivel de seguridad adicional frente al riesgo de modificación o borrado accidental de los datos origen, ya que, por defecto, con independencia de los permisos que tenga la cuenta utilizada para la conexión, ACL es únicamente de solo lectura. ACL no puede agregar, actualizar o eliminar datos del origen de datos, ni modificar un origen de datos de ninguna manera. Esta restricción se aplica a todos los orígenes de datos a los que ACL puede acceder: orígenes de datos basados en archivos, bases de datos y servicios de datos en la nube.

[17] Para obtener información detallada de los tipos de archivo, bases de datos y orígenes de datos en la nube a los que se puede conectar ACL véase https://help.highbond.com/helpdocs/analytics/151/es/Content/analytics/defining_importing_data/data_sources_you_can_access_with_acl.htm#Databases_and_cloud

Los archivos de datos de ACL (.fil) creados a partir de datos importados también son de solo lectura en ACL. ACL no puede alterar los archivos .fil, excepto por la actualización del archivo desde el origen de datos.

Los archivos .fil son totalmente independientes del origen de datos que se utiliza para crearlos. Si se elimina un archivo .fil, el origen de datos no sufre ninguna modificación.

Sin embargo, este mecanismo de obtención de la información requiere el acceso por parte del auditor a las bases de datos del ente auditado lo que, en determinadas ocasiones, puede plantear conflictos con respecto a la política de seguridad, ya que el acceso a este entorno suele estar muy limitado.

Normalmente, las herramientas ADA utilizadas por el auditor están instaladas en los equipos de trabajo del equipo de auditoría o en los sistemas corporativos del OCEX, de forma que el acceso a las bases de datos de producción del ente auditado desde un equipo o red externa puede suponer un incumplimiento de la política y normativa de seguridad.

En estos casos, el auditor junto con el personal responsable de la aplicación y de sistemas del ente auditado deben analizar posibles alternativas que den respuesta a la necesidad del auditor de ser autónomo en el acceso a los datos cumpliendo con la política de seguridad del organismo auditado. Entre las posibles opciones, se encuentra la utilización de un sistema intermedio (máquina de salto), gestionado por el ente auditado de acuerdo con su política de seguridad. En este sistema se podrían instalar las herramientas ADA, de forma que el auditor pudiese, a través de esta máquina, acceder a los bases de datos, evitando así el realizar dicho acceso de forma directa. En el ***Anexo 11 Propuesta de arquitectura para la extracción de datos desde un entorno de producción y ejemplos para su uso*** se desarrolla con más detalle esta propuesta.

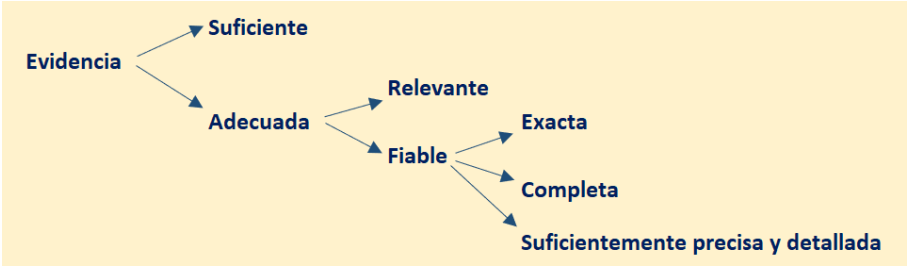
c) Descarga directa de tablas.

Si el auditado utiliza el ERP del fabricante SAP, además de los mecanismos anteriores, también se dispone de la opción de extraer los datos con la transacción *SE16* (es una transacción para mostrar información de una tabla determinada). Los detalles del uso de esta opción se describirán en el ***Anexo 10 Extracción de datos utilizando la transacción SE16 en un sistema SAP.***

15. Garantizar la fiabilidad de los datos en el proceso de su obtención y transformación

a) Fiabilidad de la información fuente

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 (ver apartados 6 a 9), la información obtenida del ente auditado que se vaya a utilizar como evidencia debe ser:



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)*.

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**[18] 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

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

información disponible y algunas son más confiables que otras.

Para verificar la fiabilidad de la fuente de información utilizada en las pruebas sustantivas el auditor tiene dos posibilidades: a) realizar un muestreo de elementos para verificar su documentación soporte para concluir si dl conjunto de datos es exacto, completo y válido; o b) revisar los controles internos asociados con la exactitud, completitud y validez de la información.

Además, se debe evaluar si la información de la entidad es suficientemente precisa y detallada para los fines de la prueba a realizar[19].

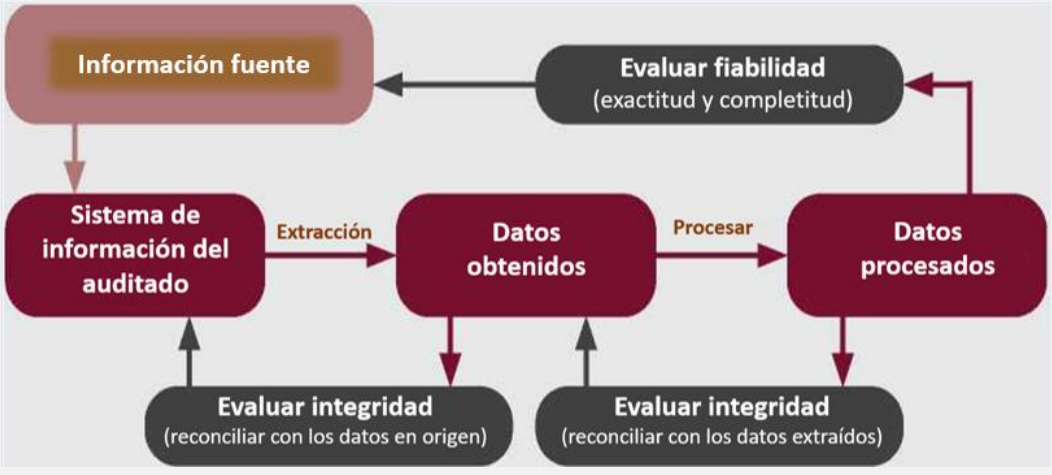
Para un OCEX, ser capaz de acceder y utilizar los datos de los fiscalizados es fundamental para la ejecución de una auditoría de calidad y es un proceso facilitado por la tecnología, que permite a los auditores obtener, almacenar y analizar datos de una manera más eficaz. Aunque hasta hace poco el proceso para obtener los datos contables de los entes auditados y otra información necesaria para la auditoría era básicamente manual, con la implantación de la administración electrónica, la forma en que los auditores acceden a los datos de los entes fiscalizados ha variado sustancialmente.

Por ello, el proceso para obtener datos, transformarlos a un formato utilizable, determinar su **integridad** y evaluar su **fiabilidad**, puede ser un reto para los auditores, y además es necesario **documentar** debidamente todo este proceso. Ambos conceptos están interrelacionados, y a los efectos de esta guía tendrán el siguiente significado:

- La **integridad** se refiere a la exactitud con la que los datos se han extraído del sistema fuente, transferidos al auditor y transformados en un formato adecuado para que el auditor los utilice en su herramienta ADA. Es decir, **la integridad debe garantizar que los datos no han experimentado alteraciones indebidas** en este proceso.
- La **fiabilidad** como acabamos de ver se refiere a la **exactitud** y **completitud** de la información fuente generada por la entidad que vaya a utilizarse como evidencia de auditoría.

Esta distinción es necesaria ya que los datos pueden tener integridad (conciliación con el lugar de recogida, no ha habido cambios en el proceso de extracción y análisis por el auditor) pero no fiabilidad (se han obtenido pruebas insuficientes sobre la exactitud y completitud de la información de la fuente de información) y el auditor debe ser consciente de los riesgos y su impacto en la auditoría.

Con un ejemplo sobre la integridad y fiabilidad de la información utilizada puede comprenderse mejor esta cuestión:



Un auditor ha extraído datos del sistema de inventario del ente auditado para llevar a cabo procedimientos relacionados con la exactitud, valoración e imputación del saldo de la cuenta de existencias y las revelaciones relacionadas. Los datos extraídos, transferidos y almacenados por el auditor se han reconciliado con el sistema de origen del auditado sin errores.

El auditor concluye que la información obtenida ha mantenido su integridad respecto del sistema del auditado.

El auditor tiene la intención de llevar a cabo procedimientos para evaluar la obsolescencia del inventario. Para determinar

[19] Ver párrafos A49 y A50 de la NIA-ES-SP 1500.

*la fiabilidad de los datos que se utilizarán como evidencia de auditoría, el auditor selecciona una muestra y prueba la exactitud y completitud de la columna de fecha de compra del conjunto de datos extraídos. El auditor identifica a partir de la muestra analizada que determinados elementos **no** coinciden con la documentación de origen.*

Por lo tanto, existen dudas sobre la fiabilidad de los datos para los fines del auditor.

(Fuente: Integrity of Data Obtained for the Purpose of an Audit of a Financial Report)

En la GPF-OCEX 1503 se profundiza en esta cuestión y debe leerse conjuntamente con la presente guía.

b) Integridad en la obtención (acceso, extracción y transferencia) de datos

El mantenimiento de la integridad de los datos obtenidos por el auditor es fundamental. Los errores que no se detecten en el proceso de extracción y transferencia de los datos pueden repercutir negativamente en la obtención de evidencias de auditoría suficientes y adecuadas para respaldar la conclusión del auditor.

El proceso de obtención de datos puede variar significativamente en función de la naturaleza y la fuente de los datos, y de una entidad a otra en las que los sistemas se han configurado de manera diferente. Es importante que el auditor establezca un proceso sólido que abarque tanto la extracción como la transferencia de los datos para mitigar algunos de los riesgos de integridad. Este proceso debe establecerse a nivel de OCEX y debe incluir la consideración de cuándo se requerirán conocimientos especializados incluyendo expertos internos o externos.

Es importante que los auditores tengan un claro conocimiento de lo que puede salir mal durante el proceso de obtención para poder ejecutarlo adecuadamente y garantizar que se mantenga la integridad de los datos.

Extracción y transferencia	¿Qué puede salir mal?	Posible mitigación
Cuestiones específicas de los datos	• Problemas con la integridad de los datos antes de la extracción. • Los datos extraídos del ente auditado se corrompen durante la transferencia. • Problemas con la integridad de los datos mantenidos por un tercero.	• Conciliación tras la extracción y transferencia de datos. • Se da a los auditores acceso directo para extraer los datos en lugar de depender del auditado. Esto dependerá del auditado y sus sistemas.
Cuestiones relativas al sistema	• Imposibilidad para extraer datos en un formato utilizable (por ejemplo, los informes solo se pueden obtener en PDF). • La extracción está incompleta o no se ejecuta. • La extracción de grandes volúmenes de datos causa fallos del sistema. • Limitaciones en cuanto a la disponibilidad de datos (determinados datos no son conservados por el sistema).	• Conocer las limitaciones de los sistemas desde el principio y trabajar con el ente auditado para identificar alternativas. • Asegurar que el ente auditado tenga un conocimiento suficiente de sus propios sistemas, lo que puede requerir conversaciones con proveedores de software. • Contactar directamente con los proveedores de software para entender cómo extraer los datos necesarios.
Quién realiza la extracción	• La falta de conocimiento del ente auditado de su sistema da lugar a la extracción de datos incorrectos (por ejemplo, parámetros incorrectos en un informe). • La falta de conocimiento del sistema por parte del auditor da lugar a la extracción de datos incorrectos. • Falta de comprensión del auditor sobre cómo funciona su herramienta ADA. • Errores técnicos que se producen cuando los datos se cargan en los sistemas del auditor. • Manipulación de datos durante el proceso de extracción y transferencia.	• Evaluación de la fiabilidad de las herramientas de extracción de datos utilizadas por el auditado. • Evaluar las capacidades y competencias del equipo de auditoría y contar con políticas claras sobre quién puede realizar tareas y cuándo se requieren expertos. • Disponer de un proceso para identificar cualquier manipulación durante el proceso de extracción y transferencia cuando el auditor no lo haya llevado a cabo.

En todo caso se deben incluir mecanismos de control de la integridad de la información extraída (totales de campos numéricos, número de registros extraídos, valores mínimo y máximo de campo fecha, etc.).

c) Integridad durante la transformación y almacenamiento de datos

En esta guía, "transformación" se utiliza para describir la forma en que los datos brutos recogidos por el auditor son tratados para su utilización (conversión de formatos cuando es necesario y carga en las herramientas ADA).

El proceso para transformar los datos en un formato utilizable y la carga de los datos transformados en las herramientas ADA a ser utilizadas por el auditor, crea una serie de ocasiones para que ocurran errores. Si este paso se hace incorrectamente, el uso de los datos y cualquier conclusión basada en los datos transformados puede ser incorrecto e impactar en la opinión del auditor.

Es importante que una vez transformados los datos se concilien con los recogidos para garantizar su integridad. El riesgo de que algo vaya mal durante la fase de transformación aumenta cuando el auditor debe realizar una gran de limpieza o depuración de datos, así como cuando realiza procedimientos manuales orientados a adaptar el formato de la información recibida con el fin de facilitar la carga o tratamiento en la herramienta ADA (por ejemplo, eliminación de saltos de línea, corrección de errores en la creación de campos por problemas con el separador de campos utilizado, etc.).

Transformación y almacenamiento	¿Qué puede salir mal?	Posible mitigación
Transformación	• Asignación incorrecta de datos y otros errores básicos durante la depuración de datos para su uso en la herramienta ADA, como la eliminación o interpretación incorrecta de información clave (por ejemplo, la eliminación de identificadores únicos para transacciones o formatos de fecha convertidos incorrectamente). • Errores en las herramientas utilizadas por el auditor, ya sea porque los scripts no funcionan como estaba previsto o errores al cargar los datos en las herramientas del auditor, como el cambio de columnas o caracteres especiales que crean problemas. Las herramientas pueden requerir conocimientos que exceden los de los auditores que las utilizan.	• Disponer de una documentación clara y completa del modelo de datos. • Realizar procedimientos para identificar errores en la estructura de los datos o de otro tipo una vez que se carga en las herramientas ADA del auditor. • Tener las conocimientos y competencias adecuadas en el equipo de auditoría para poder entender la transformación y revisarla adecuadamente. • Incluir mecanismos de control de la integridad de la información extraída (totales de campos numéricos, número de registros extraídos, valores mínimo y máximo de campo fecha, etc.).
Almacenamiento de los datos transformados	• Los datos una vez transformados se alteran	• Disponer de procedimientos claros sobre cómo gestionar los datos una vez extraídos y transferidos del sistema del auditado para mantener la integridad (p.e. restringir el acceso solo al personal autorizado).

d) Validación de la información obtenida

Una vez obtenidos los datos, se realizarán comprobaciones para asegurar que la información se corresponde con la solicitada y es la necesaria para la consecución de los objetivos y que no hay problemas de integridad. Al menos se realizarán las siguientes validaciones:

- Comprobación del número de registros y de la suma de control.
- Recuento de registros (estimación de si es una cifra razonable).
- Comprobación de secuencias (que no falte ningún número en un campo que sea secuencial).
- Comprobación de fechas (fechas que deban estar comprendidas en un periodo).

De manera general, los principales objetivos de las pruebas para validar la información recibida, junto con las preguntas que debemos contestar en el análisis de cada objetivo, son las siguientes:

Objetivo	Preguntas que hay que contestar
Validez	• ¿Todos los campos están correctamente definidos? • ¿Hay algún dato corrupto?
Totales de control	• ¿Los recuentos de registros se concilian con los totales de control? • ¿Los valores numéricos coinciden con los totales de control?
Límites	• Para los campos numéricos y de fechas, ¿los valores están dentro de los límites?
Calidad y completitud	• ¿Hay caracteres en blanco? • ¿Los valores siguen el formato adecuado? • ¿Existen "huecos" en campos que deberían ser secuenciales?
Unicidad	• ¿Hay algún campo o registro duplicado?
Razonabilidad	• ¿La distribución de valores es razonable? • ¿Los valores negativos/nulos son razonables?

El objetivo de estas pruebas es verificar si los datos recibidos son correctos o, por el contrario, contienen algún tipo de error. Por ejemplo, si algún campo que siempre debe tener contenido está vacío, si un campo numérico contiene textos, si algún campo tipo fecha no tiene ese formato, si se utiliza la coma y el punto decimal indistintamente, etc. Algunos de estos errores pueden ocasionar resultados incoherentes.

Si surgen muchos errores de estos tipos deberemos cuestionarnos la calidad de los datos utilizados y su fiabilidad. (ver ***Anexo 14 Cómo tratar las excepciones al usar ADA en determinados procedimientos sustantivos***).

16. ¿Dónde se almacenarán los datos obtenidos y cómo se mantendrá su integridad?

Es importante determinar dónde se almacenarán los datos una vez obtenidos y cómo se mantendrá su integridad una vez que estén bajo el control del auditor.

Las normas legales exigen que los OCEX establezcan políticas y procedimientos para mantener la confidencialidad, la custodia segura y la integridad de la documentación de auditoría, así como tener políticas de retención apropiadas para esa documentación.

Si bien las normas técnicas y los requisitos éticos pertinentes abordan la documentación de la auditoría, es importante que los auditores establezcan normas internas para conservar datos que no forman parte de los papeles de trabajo. Los auditores deben tener en cuenta cuestiones tales como:

- ¿Tiene el OCEX la competencia legal para para recopilar y almacenar los datos?
- ¿Cómo mantendrá el OCEX la seguridad sobre los datos?
- ¿Se utilizará un tercero para almacenar datos?
  - Cuando se utiliza un tercero, ¿cuáles son los acuerdos en torno al acceso, las copias de seguridad y la retención con el tercero?
  - ¿Cómo mantiene el tercero la seguridad sobre los datos?
  - ¿Dónde se almacenarán los datos por el tercero? ¿Los datos serán transfronterizos?
- ¿Existen políticas de conservación y destrucción adecuadas para los datos recopilados que no forman parte de los papeles de trabajo?
- ¿Tiene el OCEX un DPD?
- ¿Tiene el OCEX un plan en caso de violación de datos?
- ¿Dispone el OCEX un plan de formación adecuada en materia de tratamiento de datos para que el personal comunique la importancia de un tratamiento seguro de los datos de los auditados?

IV DISEÑO Y EJECUCIÓN DE LAS PRUEBAS

17. Archivo de la información recibida (*ejemplo con ACL*)

Cuando estemos en la sede del ente auditado, la información obtenida se ubicará siempre en una zona cifrada del ordenador portátil del auditor que realice la prueba, en una carpeta cuya estructura sea:

NOMBREENTIDAD**\Archivos originales remitidos**

Para trabajar la información con ACL haremos una copia de los ficheros originales, que almacenaremos dentro de la carpeta de ACL, en una subcarpeta llamada "Ficheros originales". Las tablas de ACL (resultado de la importación en ACL de los datos origen), así como los scripts y demás información creada durante el trabajo se ubicará en la carpeta "Ficheros proyecto".

Los resultados (Excel, Word, etc..) obtenidos en el proyecto de ACL se guardarán en la carpeta "Resultados".

Por tanto, mientras se realiza el trabajo de campo fuera del OCEX, la estructura de carpetas (que se almacenará en la zona encriptada) será la siguiente:

NOMBREENTIDAD**\Archivos originales remitidos**
NOMBREENTIDAD**ACL\Ficheros originales**
NOMBREENTIDAD**ACL\Ficheros proyecto**
NOMBREENTIDAD**ACL\Resultados**

Cuando se trabaje en las instalaciones del OCEX, la estructura de carpetas de cada equipo en el servidor debe tener el contenido mínimo siguiente:

…\PAA2022\NOMBREENTIDAD\ **Archivos originales remitidos**
…\PAA2022\NOMBREENTIDAD**ACL\Ficheros originales**
…\PAA2022\NOMBREENTIDAD**ACL\Ficheros proyecto**
…\PAA2022\NOMBREENTIDAD**ACL\Ficheros Resultados**

Al finalizar el trabajo de campo y tras su volcado al servidor, deben eliminarse todos los ficheros de los ordenadores portátiles.

18. Codificación de la prueba

Dentro del proyecto de ACL, los ficheros de datos se agruparán en dos carpetas, "Tablas_Iniciales[20]" y "Tablas_Proyecto" que, a su vez, podrán desglosarse en subcarpetas en función de su finalidad. En "Tablas_Iniciales" se introducirán las tablas originales y en "Tablas_Proyecto" todas las restantes. Las tablas, en una y otra carpeta, se nombrarán utilizando las siguientes reglas para documentar la información del proyecto:

- **TABLAS ORIGINALES:**

Nombre tabla original: ***<Letra mayúscula>* + "00" + *<Nombre descriptivo>*** **(ej. A00_Facturas)**

Las *tablas originales* importadas a ACL comenzarán por una letra mayúscula seguida de dos ceros, de forma que todas las tablas originales serán identificables por esta característica.

A continuación, se añadirá al nombre de la tabla un guion bajo y un nombre descriptivo. Si el nombre de la tabla original es suficientemente descriptivo lo mantendremos y en caso contrario lo renombraremos (en estos casos se debe conservar, en un documento Word o Excel, las **correspondencias** de los ficheros originales con las tablas de ACL), por ejemplo:

- ✓ A00_Pedidos
- ✓ B00_Facturas
- ✓ P00_MovimientosContables

[20] Los nombres de las carpetas dentro de un proyecto de ACL no pueden llevar espacios. Si se introducen espacios al crear la carpeta o renombrarla, ACL los sustituye directamente por el carácter "_"

En caso de que en un proyecto se llegue a la codificación Z00_nombre_descriptivo y sea necesario cargar más tablas originales, se continuará de la siguiente forma:

- ✓ **AA00**_Nombre_descriptivo
- ✓ **BB00**_Nombre_descriptivo

- **TABLAS INTERMEDIAS:**

Nombre tabla intermedia: **"T" + <_Dos dígitos_> + "_" <Letra de la/s tabla/s origen utilizada> + "_"+ <_Nombre descriptivo_>** **(ej. T05_A_*Facturas*)**

Las ***tablas intermedias o finales*** en las que se ha realizado alguna extracción o se han añadido datos de otras tablas, se denominarán comenzando por un guion bajo[21] más un número secuencial (que seguirá el siguiente patrón: 05, 10, 15, etc.)) seguido de la misma letra de la tabla de origen utilizada (si provienen de dos tablas se utilizarán las letras de las dos tablas) y a continuación, el nombre descriptivo de la tabla, todo ello separado por guiones.

Los intervalos de 5 unidades servirán para que se puedan intercalar tablas en medio con los dígitos 01, 02, 03, 04, 06, 07, 08 y 09.

Ejemplos_

- ✓ T05_A_PedidosValencia
- ✓ T10_B_Facturas2021
- ✓ T15_AB_PedidosValenciaFacturados2021

NOTA: Cuando se indica AB, se refiere a una unión de los ficheros origen A y B, donde A es el primario y B el secundario

En aquellos trabajos en los que exista un elevado número de pruebas o de mayor complejidad, resulta aconsejable un mayor nivel de codificación. Por ejemplo, una posibilidad es introducir la codificación "Px", (donde x=número de la prueba) en lugar de la letra "T", consiguiendo así que las tablas se muestren de forma ordenada según la prueba a la que correspondan. De esta forma, los nombres de las tablas quedarían:

- ✓ P1_05_A_PedidosValencia
- ✓ P1_10_B_Facturas2021
- ✓ P1_15_AB_PedidosValenciaFacturados2021
- ✓ P2_05_P_MovimientosContables2021
- ✓ P2_10_BP_FacturasContabilizadas2021
- ✓ P2_15_BP_Facturas2021NoContabilizadas

- **SCRIPTS:** La denominación de los scripts se iniciará con la letra "S" seguida de dos dígitos y a continuación un nombre descriptivo de la funcionalidad del script.

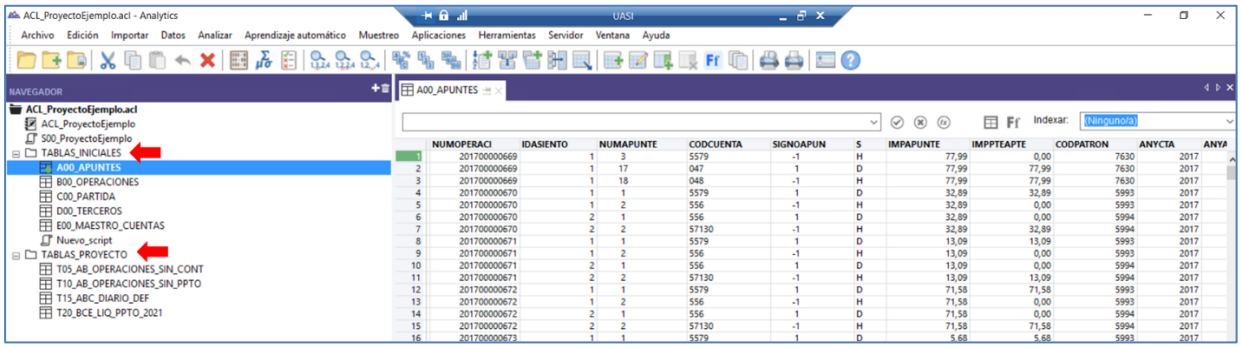
Nomenclatura scripts: **"S" + <Dos dígitos> + <Descripción de la prueba>** ***(ej: S00_CuadrarContabilidad)***

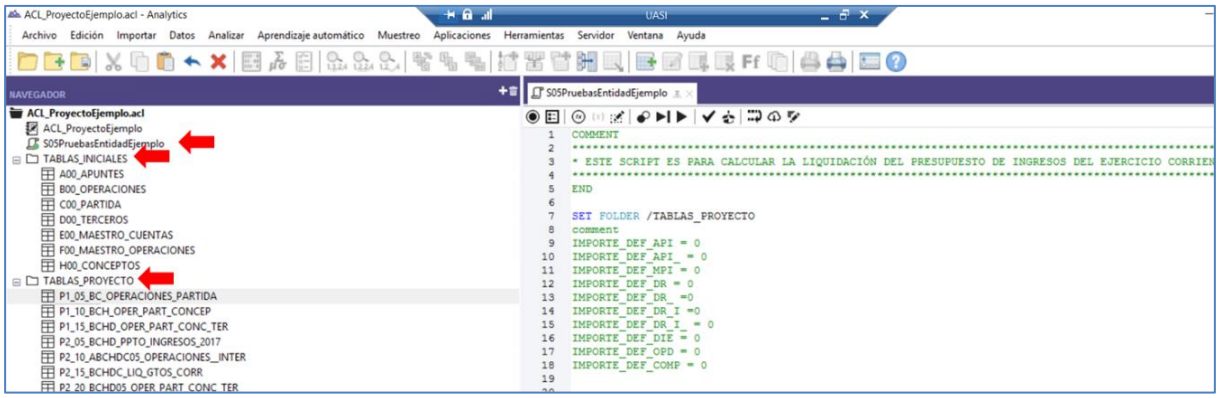
Los siguientes ejemplos ilustran el patrón de nomenclatura propuesto:

- ✓ S00_CargaDatos
- ✓ S05_TratamientosIniciales
- ✓ SXX_ResultadoFinal

[21] Se incluye un guion bajo al comienzo del nombre de la tabla, porque ACL no permite comenzar con un número.

En la siguiente figura se adjuntan dos ejemplos de cómo quedaría organizado un proyecto de ACL utilizando la estructura de codificación descrita en esta sección.





<u>Nomenclatura para pruebas de datos complejas</u>

En aquellos casos en los que exista un elevado volumen de pruebas o la complejidad de éstas lo haga aconsejable, se seguirá la siguiente estructura y nomenclatura.

- **ESTRUCTURA del proyecto de ACL:** Se crearán las siguientes carpetas:
  - A_Tablas originales: Contendrá únicamente las tablas originales del proyecto, siguiendo la nomenclatura descrita en el apartado anterior.

    Ejemplo: A00Facturas, B00MovimientosContables, etc.
  - B_Pruebas: Se creará una subcarpeta para cada prueba, que contendrá tanto las tablas intermedias obtenidas durante la prueba como los scripts correspondientes.
    - Prueba01
    - Prueba02
    - …
- **TABLAS ORIGINALES:** Se seguirá el mismo patrón de la sección anterior, es decir, el nombre de la tabla empezará con una letra mayúscula, seguida de dos ceros y un nombre descriptivo de la tabla.

Nombre tabla original: ***<Letra mayúscula> + "00" + <Nombre descriptivo>*** ***(ej. A00_Facturas)***

- **TABLAS INTERMEDIAS:**

Nombre tabla intermedia: **<Código Prueba (P1, P2…)>+ <dos dígitos (05,10…)>+<Nombre descriptivo>"** ***(ej. P1_05_Facturas2022)***

Siguiendo el ejemplo anterior:

- P1_05_Facturas2022
- P1_05_RestoFacturas
- P1_10_ClientesValencia
- P1_10_RestoClientes
- P1_15_CruzanFacturasclientes
- P1_15_NxFacturasclientes
- P1_15_NxClientesFacturas

- **SCRIPTS:**

  Como se ha indicado, los scripts utilizados para codificar cada prueba se guardarán en la carpeta de la prueba correspondiente. A la hora de nombrar los scripts, se seguirá el siguiente criterio:

  Nomenclatura scripts:
  "S" + <Número de la prueba> + <Descripción de la prueba>
  (ej: SP1_CuadrarContabilidad)

Incorporación de validaciones en las pruebas

Es una **buena práctica que se debe cumplir con carácter general** para controlar el correcto diseño y ejecución de la prueba en ACL/IDEA **obtener tablas de registros no utilizados en todos los análisis** en los que se desprecian determinados registros de las tablas utilizadas. Por ejemplo:

- En una selección realizada mediante un filtro, obtener además de los registros que cumplen la condición de filtrado, una tabla que incluya los registros restantes, y comprobar que la suma del número de registros de ambas tablas es igual al número de registros de la tabla original.
- En un cruce entre dos tablas, obtener la tabla resultante del cruce, junto con dos tablas más, que recojan los registros de las tablas iniciales que no han cruzado.

19. Automatización de las pruebas: Scripts

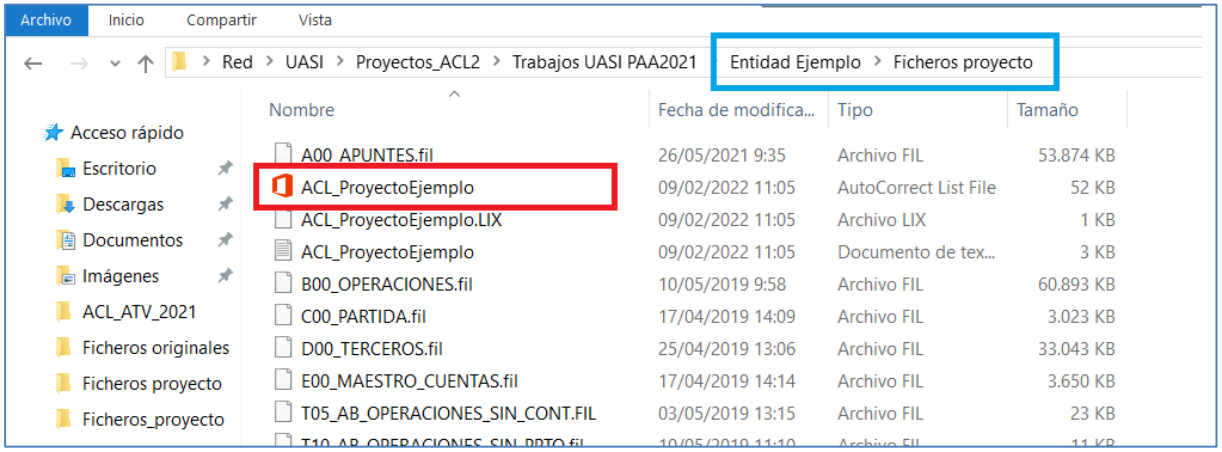
Con objeto de documentar las pruebas y automatizarlas, se registrarán los scripts (registro de todas las instrucciones ejecutadas en las pruebas), de forma que estos scripts puedan ser reutilizados en otras pruebas similares de otras entidades o en la misma entidad en ejercicios sucesivos.

Las reglas para la nomenclatura de los scripts utilizados, de forma que el trabajo quede adecuadamente documentado y facilite su posterior revisión y reutilización, son las expuestas en el apartado anterior sobre codificación de la prueba.

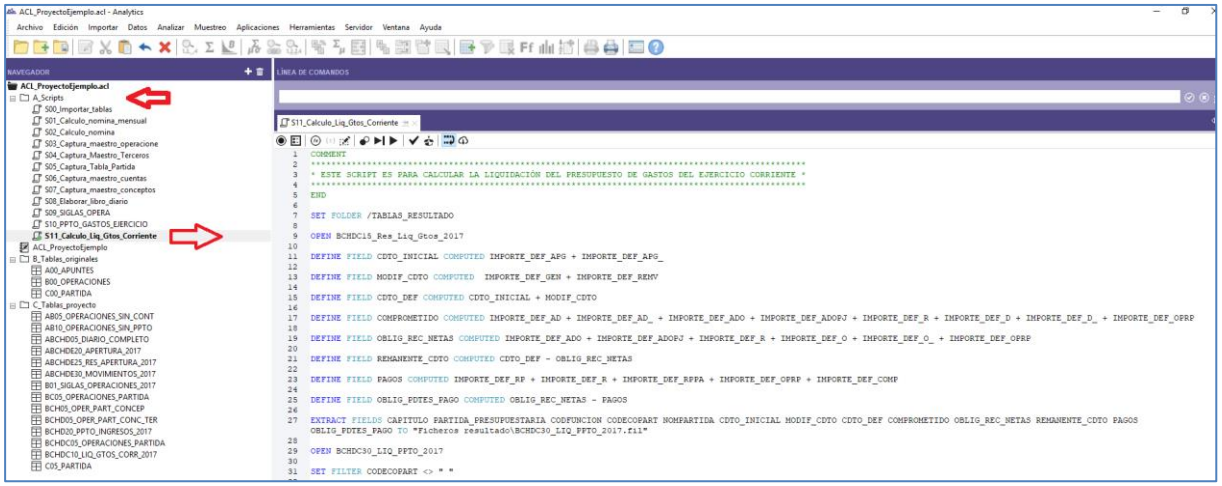
- En pruebas complejas o largas, a veces resulta conveniente elaborar un último Script que ejecute todos los anteriores (comando "do" seguido del nombre del script a ejecutar).
- Paralelamente, cabe destacar que una de las ventajas de trabajar con herramientas de análisis de datos, en este caso ACL, es que las comprobaciones y análisis realizados quedan automáticamente documentados.

  En concreto, en caso de utilizar ACL, no es necesario trasladar manualmente el contenido de los scripts a documentos Word y/o ficheros. El archivo del proyecto ACL contiene toda la estructura del proyecto - carpetas creadas, nomenclatura de las tablas (sin su contenido, es decir, sin los datos), los scripts, etc. Para documentar las pruebas realizadas (qué tratamientos y análisis se han hecho sobre los datos originales) basta con guardar una copia de dicho fichero.

  El archivo del proyecto ACL tiene la forma "***Nombre del proyecto*.acl**", y si se trabaja con la estructura de carpetas explicada anteriormente, éste se encuentra en la carpeta "ficheros de proyecto".



Si abrimos el archivo anterior, éste contiene toda la información de los scripts y la estructura de carpetas y tablas del proyecto. Por tanto, las pruebas realizadas quedan automáticamente documentadas.



- Finalizado el trabajo, se almacenará una copia del proyecto ACL (fichero *.ACL) en el *Archivo Permanente*.

20. Análisis de los resultados obtenidos y conclusiones

Una vez obtenidas las tablas finales, se procederá a realizar el análisis de la información obtenida y elaborar las conclusiones pertinentes.

A estos efectos, se documentará en un Excel los resultados y las conclusiones que se hayan obtenido, detallando:

- Los resultados y conclusiones obtenidas a partir del análisis de los datos realizado en la prueba.
- Explicación todas las diferencias que surjan.
- Comentarios a los resultados del responsable del ente auditado.

Los documentos (Excel, Word, etc.) que recojan las conclusiones de la prueba se guardarán en la carpeta de *"Resultados"* indicada en el apartado anterior (zona encriptada de los portátiles (de forma temporal, cuando se esté trabajando fuera de las instalaciones del OCEX y, posteriormente, en el servidor).

Un problema común para los auditores que utilizan ADA en determinados casos de procedimientos sustantivos es el volumen de valores atípicos que pueden generarse al aplicar tales herramientas para analizar poblaciones, especialmente cuando se utilizan en una población por primera vez. Para profundizar en cómo tratar estos casos ver en ***Anexo 14 Cómo tratar las excepciones al usar ADA en determinados procedimientos sustantivos***.

II DOCUMENTACIÓN DE LA PRUEBA

21. El uso de ADA y la documentación del auditor de acuerdo con las NIA-ES-SP

Este apartado de la guía tiene por objeto ayudar a los auditores a comprender cómo el uso de ADA durante una auditoría puede afectar a su documentación de conformidad con la NIA-ES-SP 1230 y prestar asistencia práctica sobre cómo documentar este tipo de pruebas.

Esta guía no modifica ni anula las NIA-ES-SP/GPF-OCEX, ni su lectura sustituye a la lectura de la GPF-OCEX/MFSC 1220 o la NIA-ES-SP 1230. Los ejemplos se ofrecen únicamente con fines ilustrativos.

La NIA-ES-SP 1230 no distingue entre el uso de herramientas y técnicas automatizadas y las manuales con respecto a los requisitos de documentación de auditoría, pero el uso de HTA/ADA puede dar lugar a diferentes consideraciones sobre la documentación.

La NIA-ES-SP 1230 se basa en principios y, por lo tanto, **sigue siendo aplicable independientemente de la naturaleza de la herramienta o técnica que aplique el auditor.**

Por ejemplo, la **naturaleza y propósitos de la documentación de auditoría** enunciados en los párrafos 2 y 3 de la NIA-ES-SP 1230 son los mismos, independientemente de si se utilizan HTA/ADA para llevar a cabo la auditoría, e incluyen lo siguiente:

- Evidencia de las bases del auditor para llegar a una conclusión sobre el cumplimiento de los objetivos globales de la auditoría.
- Evidencia de que la auditoría se planificó y ejecutó de conformidad con las NIA-ES-SP y los requerimientos legales o reglamentarios aplicables.
- Ayudar al equipo de auditoría a planificar y realizar la auditoría.
- Ayudar a los miembros del equipo de auditoría responsables de la supervisión en la dirección y supervisión del trabajo de auditoría y el cumplimiento de sus responsabilidades de revisión de conformidad con la GPF-OCEX/MFSC 1220.
- Permitir que el equipo de auditoría rinda cuentas de su trabajo.
- Mantener un archivo de cuestiones de importancia permanente para las auditorías futuras.
- Realizar revisiones de control de calidad e inspecciones de conformidad con la GPF-OCEX/MFSC 1220
- Permitir la realización de inspecciones externas de conformidad con la GPF-OCEX/MFSC 1220.

En el ***Anexo 12 El uso de HTA y la documentación del auditor de acuerdo con las NIA-ES-SP*** se realizan diversas consideraciones sobre cómo aplicar la NIA-ES-SP 1230 cuando se usa HTA.

De manera concreta, cuando el auditor realice utilizando herramientas ADA pruebas complejas o muy extensas, deberá completarse el papel de trabajo indicado en el ***Anexo 13 Modelo para documentar una prueba de datos***. En él se recoge una ficha con los datos generales más significativos junto con un catálogo numerado de las pruebas a realizar.

22. Contenido de la documentación de una prueba de datos

El trabajo realizado en una prueba de datos debe ser debidamente documentado y supervisado, como cualquier otro trabajo de auditoría.

Cuanto más compleja sea la prueba más detallada debe ser su documentación. Por el contrario, pruebas sencillas requerirán una documentación más simple.

a) Contenido general de la documentación de una prueba de datos

La documentación de la prueba de datos, normalmente, incluirá la siguiente documentación:

- Objetivos de la prueba

- Resumen de las principales reuniones mantenidas en relación con la obtención de los datos, el diseño y evaluación de los resultados de la prueba.
- Escritos de solicitud de los datos necesarios o las instrucciones para su obtención.
- La naturaleza y la fuente de los datos, incluida la identificación de las características que pueden incluir:
    - El tipo de datos.
    - El sistema del que se recogieron los datos.
    - El modelo de datos. Descripción del modelo de datos o bases de datos del sistema de información.
    - Las tablas concretas de la base de datos o los informes utilizados para obtener los datos.
- Cómo se extrajeron los datos, incluyendo:
    - La fecha en que se produjo la extracción.
    - ¿Quién realizó la extracción?
        - Están debidamente capacitados para llevar a cabo la extracción.
        - Cuando se utiliza un experto, señalar si el experto es interno o externo.
    - El método de extracción, incluidas las herramientas utilizadas. ¿Cómo se determinó que las herramientas utilizadas eran las adecuadas?
    - El método de transferencia de los datos al auditor, incluidas las herramientas utilizadas. ¿Cómo ha asegurado el auditor que los datos **no han sido manipulados** durante el proceso de transferencia de los datos al auditor?
    - Evaluación de la **exactitud y completitud** de los datos extraídos de la fuente para poder concluir sobre la **integridad de los datos** obtenidos.
- Cómo se transformaron los datos, incluyendo:
    - ¿Quién realizó la transformación?
        - Están debidamente capacitados para llevar a cabo la transformación.
        - Cuando se utiliza un experto, señalar si el experto es interno o externo.
    - El método de transformación, incluidas las herramientas utilizadas. ¿Cómo se determinó que las herramientas utilizadas eran las adecuadas?
    - Evaluación de que la **integridad** de los datos se ha mantenido a lo largo del proceso de transformación.
- Dirección, supervisión y revisión de los miembros del equipo de auditoría.
- Cómo mantiene el auditor la integridad de los datos después del proceso de recogida y transformación (archivo y almacenamiento).
- Scripts utilizados o historia de las tablas finales con los resultados (opción de ACL para documentar las pruebas) o bien directamente, el fichero ACL del proyecto.
- Diagramas de flujo de la prueba.
- Hoja de Excel/Word con las conclusiones y resultados obtenidos.

Toda esta documentación se incorporará al sistema de Papeles Electrónicos de Trabajo (PET) de la fiscalización correspondiente como evidencia para soportar las conclusiones obtenidas.

Aunque puede haber problemas en la determinación de cómo documentar la extracción, transferencia y transformación de los datos, es importante que los auditores tengan presente que, si bien el volumen de datos recopilados por los auditores ha aumentado mucho, la documentación requerida no ha cambiado. No es necesario incluir poblaciones enteras de datos como parte de la documentación de auditoría.

Todos los conjuntos de datos recopilados y que no formen parte de la documentación de auditoría deben estar debidamente securizados y aplicárseles las políticas de retención y borrado adecuadas aprobadas por la Política de Seguridad de la Información del OCEX. Aunque estos conjuntos completos de datos pueden no formar parte de la documentación de auditoría, la documentación de su recogida y transformación sí que debe formar parte de la documentación de auditoría.

Se incluirá en el **archivo permanente** de la entidad 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 (o fichero ACL del proyecto), etc.

Es importante destacar que **nunca** se debe dejar en el archivo permanente las tablas con los datos originales o de la información del proyecto de ACL, por el riesgo de accesos no autorizados, además de no ser necesario.

Las carpetas conteniendo los datos que se han archivado según los criterios expuestos en el apartado 17 puesto que son muy "pesadas" para guardarlas en el sistema de PET, se traspasarán al finalizar el trabajo al **archivo histórico** de las fiscalizaciones, según la política al respecto del OCEX (no confundir el archivo permanente con el archivo histórico).

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, con un conocimiento medio de la herramienta utilizada, 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 seguir estrictamente los criterios de estandarización del trabajo recogidos en esta guía.

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 crearon, ejecutaron y documentaron la prueba.

Una buena documentación de la prueba de datos realizada permite:

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

b) Elaboración de un diagrama de flujo con el diseño y ejecución de la prueba

De forma paralela a la ejecución de la prueba de datos deberemos elaborar el diagrama de flujo en el que se detallen los diferentes pasos hasta la obtención del fichero final con los resultados de la prueba.

Los diagramas de flujo son representaciones gráficas de las distintas fases de ejecución de una prueba de datos que permiten visualizar los filtros o selecciones de registros realizados en cada una de las fases hasta llegar al resultado final.

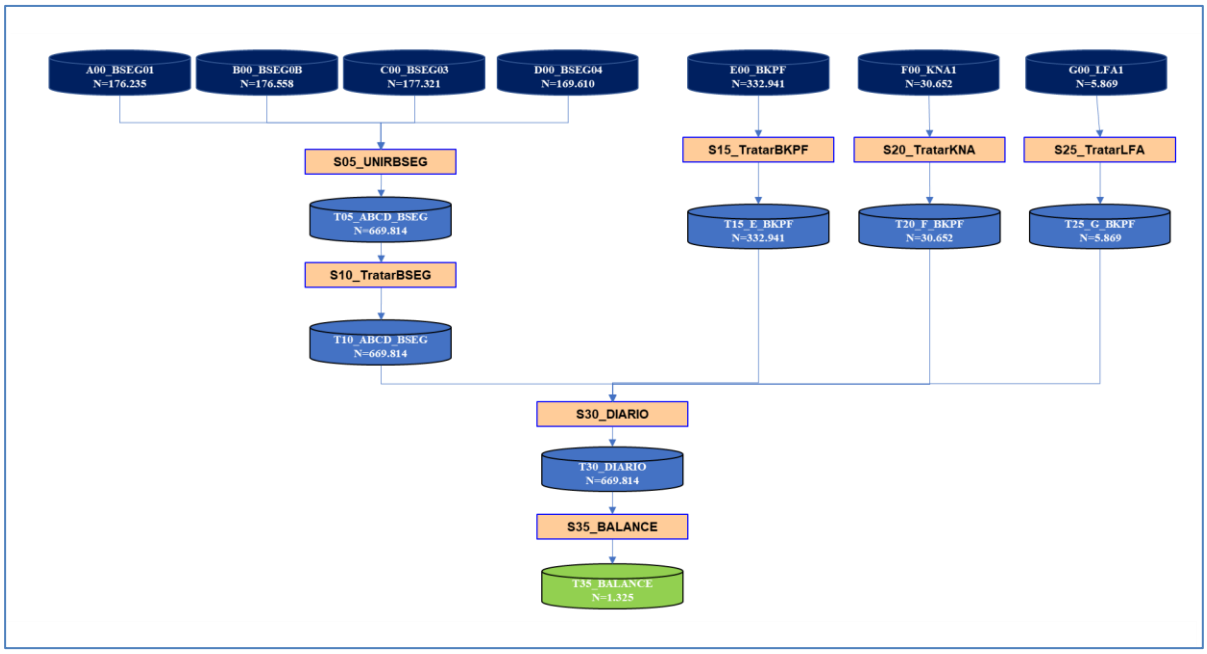
En los diagramas de flujo de la prueba se utilizarán los siguientes símbolos y códigos de colores:

Tablas origen de datos	Nombre_Tabla N=nº de registros	Resultado conforme	Nombre_Tabla N=nº de registros
Tablas intermedias	Nombre_Tabla N=nº de registros	Resultado no esperado o con incidencias	Nombre_Tabla N=nº de registros
Tablas intermedias sin uso posterior y sin incidencias	Nombre_Tabla N=nº de registros	Unión de tablas y/o scripts	→
Script	Nombre del script		

En las tablas se debe señalar el número de registros con objeto de hacer una sencilla comprobación de integridad de los datos tras la ejecución de cada script.

Ejemplo de diagrama de flujo de una prueba de datos

A continuación, se detalla un ejemplo sencillo de diagrama de flujo de una prueba (en un sistema SAP ECC 6):



Cada tratamiento realizado debe tener un punto de control.

- Cruce: Cruzan / No Cruzan Primario / No Cruzan Secundario.
- Filtrado: Además de obtener registros seleccionados, generar tabla de «no seleccionados».
- Fechas: Rangos esperados en Días / Meses / Años

Explicación del flujograma:

Debido al tamaño de la tabla BSEG, que contiene los asientos contables, la entidad la ha extraído y entregado en 4 partes (A00_BSEG01, B00_BSEG02, C00_BSEG03 y D00_BSEG04).

Todas estas tablas (A00_BSEG01, B00_BSEG02, C00_BSEG03 y D00_BSEG04) se unen mediante la ejecución del script S01_UNEBSEG dando lugar a la tabla T05_ABCD_BSEG. Esta tabla recoge los detalles de todos los asientos contables del ejercicio. Mediante el script S10_TratarBSEG se da formato a los campos de la tabla, obteniendo la tabla T10_ABCD_BSEG.

Asimismo, se da formato al resto de tablas originales, mediante la ejecución de los scripts S15_TratarBKPF, S20_TratarKNA y S25_TratarLFA.

Una vez unificada y formateada, T10_ABCD_BSEG se une con las tablas auxiliares, ya formateadas, T15_E_BKPF y T20_F_BKPF (que contienen los detalles de clientes y proveedores) y con la otra tabla de información contable T25_G_BKPF (que contiene la cabecera de los asientos contables) para obtener la tabla T30_DIARIO, mediante la ejecución del script S30_DIARIO. Todas estas tablas son tablas intermedias.

A continuación, se obtiene la tabla final T35_BALANCE mediante la ejecución del script S35_BALANCE, que permite generar el balance de sumas y saldos, y que no es más que un resumen por cuentas de todos los asientos del diario. A partir de aquí se podrá comprobar con Excel si a partir de los asientos de diario se obtiene el balance y la cuenta de pérdidas y ganancias de las cuentas anuales fiscalizadas.

Junto al nombre de cada tabla se indica el número de registros que contiene, lo que permite comprobar que el resultado intermedio o final es acorde con lo esperado.

Ver también el ***Anexo 13 Modelo para documentar una prueba de datos***.