

---

## Guía práctica de fiscalización de los OCEX

### GPF-OCEX 1971 Guía de auditoría del área de ingresos por tributos

Referencia: GPF-OCEX 1315 Revisada, NIA-ES-SP 1330, GPF-OCEX 5330 y GPF-OCEX 5340  
ISSAI-ES 400 y GPF-OCEX 4000.

*Documento elaborado por la Comisión Técnica de los OCEX  
y aprobado por la Conferencia de Presidentes de ASOCEX el 11/12/2024.*

---

1. **Introducción y objetivos de la guía**
2. **Ámbito subjetivo de aplicación**
3. **Ámbito objetivo de aplicación**
4. **Objetivos de la auditoría del área**
5. **Obtención de conocimiento del proceso de gestión tributaria y de la aplicación TI que lo soporta**
6. **Identificación de los riesgos de incorrección material**
7. **Identificación de los controles de procesamiento de la información relevantes**
8. **Evaluación del diseño e implementación (D+I) de los CPI relevantes**
9. **Valoración del riesgo de control**
10. **Revisión y evaluación de los CGTI: factores de riesgo a considerar**
11. **Revisión de la eficacia operativa de los CPI relevantes**
12. **Segregación de funciones**
13. **Análisis de las interfaces y de los controles sobre ellas**
14. **Revisión del cumplimiento legal**
15. **Importancia relativa**
16. **Procedimientos y programas de auditoría**
17. **Colaboración de expertos en auditoría de sistemas de información**
18. **Evaluación de las deficiencias de control interno detectadas**
19. **Recomendaciones**
20. **Documentación del trabajo**

Anexo 1 Documentación del conocimiento del proceso de gestión tributaria

Anexo 2 Programa de auditoría

#### 1. Introducción y objetivos de la guía

Las NIA-ES-SP tienen implícito un concepto fundamental: el auditor, al planificar una auditoría, debe identificar y valorar los riesgos de auditoría que pueden existir al ejecutar el trabajo y emitir su informe; teniendo en cuenta ese análisis, debe diseñar un conjunto equilibrado de procedimientos de forma que los riesgos queden reducidos a un nivel aceptable a la hora de emitir el informe de auditoría.

Este enfoque de auditoría basado en el análisis de los riesgos (o enfoque de riesgo) debe aplicarse al conjunto de la auditoría y con especial cuidado profesional en aquellas áreas más significativas o en aquellas cuyos riesgos inherentes sean típicamente altos, como es el caso de los ingresos tributarios. Los ingresos por tributos de una entidad son el resultado de la agregación de un gran número de transacciones de importes muy variados, que de ordinario se gestionan con sistemas de información cada vez más complejos, automatizados e integrados.

En estas situaciones, especialmente **en las entidades de tamaño mediano o grande, llegar a una conclusión u opinión de auditoría (favorable, con salvedades, denegada o desfavorable) sólo con pruebas sustantivas es, en la práctica, imposible**, siendo preciso confiar en los controles de procesamiento de la información, automatizados en su mayor parte o TI dependientes, implantados en la aplicaciones TI de gestión tributaria que ha diseñado e implantado la entidad y, por tanto, deben hacerse pruebas de auditoría sobre el diseño, implementación y eficaz funcionamiento de los controles de procesamiento de la información (CPI) y de los controles generales de tecnologías de TI (CGTI) que los respaldan.

Esta guía es aplicable en las **auditorías financieras y de cumplimiento** del área de ingresos tributarios y su **objetivo** es ayudar al auditor a:

- Adquirir un conocimiento profundo de los procedimientos/procesos de gestión establecidos por la entidad para iniciar, autorizar, registrar, procesar e informar en las cuentas anuales de los tipos de transacciones significativas relacionadas con los ingresos tributarios, desde que tiene lugar el hecho imponible hasta que se recauda el tributo y también la gestión de devoluciones de ingresos indebidos.
- Identificar y valorar los riesgos inherentes existentes en las afirmaciones relacionadas y determinar cuáles son riesgos significativos.
- Identificar, analizar y revisar el adecuado diseño, implementación y funcionamiento operativo de los CPI relevantes que abordan los riesgos inherentes significativos existentes.
- Identificar los CGTI que respaldan los CPI relevantes y revisar su adecuado diseño, implementación y funcionamiento operativo.
- Diseñar las pruebas de auditoría más adecuadas para probar la eficacia del diseño y el funcionamiento de los controles relevantes.
- Establecer los procedimientos mínimos recomendados para la fiscalización del área de ingresos tributarios, incluyendo un contenido orientativo del programa de auditoría. Incluirá cuestiones de auditoría financiera y de cumplimiento legal.
- Documentar los procedimientos ejecutados, la evidencia obtenida y las conclusiones alcanzadas.

La adecuada comprensión de esta guía **requiere el conocimiento previo de las GPF-OCEX 1315R, 5330 y 5340**. La GPF-OCEX 5340 incluye un apartado de **definiciones** que también es aplicable a la presente guía.

## 2. Ámbito subjetivo de aplicación

Esta guía está diseñada para la fiscalización de administraciones públicas que gestionan y recaudan tributos y aplican el PGCP<sup>1</sup>.

En las entidades de menor tamaño podrá limitarse la aplicación de determinados procedimientos si a juicio del auditor resulta más eficiente y se alcanzan igualmente los objetivos de auditoría.

## 3. Ámbito objetivo de aplicación

La presente guía es aplicable a la auditoría del proceso de gestión, liquidación, recaudación e inspección de ingresos tributarios<sup>2</sup> (tasas, contribuciones especiales e impuestos, tanto directos como indirectos). Por tanto, no será de aplicación ni al resto de ingresos de derecho público no tributario (como, entre otros y sin ánimo de exhaustividad, las prestaciones patrimoniales públicas no tributarias<sup>3</sup>, los precios públicos<sup>4</sup>, las multas o las subvenciones y transferencias recibidas), ni a los ingresos de derecho privado (intereses de cuentas bancarias, rendimientos obtenidos en el arrendamiento de inmuebles patrimoniales, etc)

---

<sup>1</sup> Las menciones al PGCP deben entenderse referidas a la regulación contable correspondiente del marco jurídico español del sector público que resulte aplicable en cada caso.

<sup>2</sup> Según definición contenida en el artículo 2 de la Ley 58/2003, de 17 de diciembre, General Tributaria (LGT), “*Los tributos son los ingresos públicos que consisten en prestaciones pecuniarias exigidas por una Administración pública como consecuencia de la realización del supuesto de hecho al que la ley vincula el deber de contribuir, con el fin primordial de obtener los ingresos necesarios para el sostenimiento de los gastos públicos*”. Este mismo artículo clasifica los tributos en tasas, contribuciones especiales e impuestos, incorporando la definición técnica de cada uno de estos.

<sup>3</sup> Según redacción dada a la DA 1ª de la LGT y al artículo 20.6 del Real decreto legislativo 2/2004, de 5 de marzo, que aprueba el Texto Refundido de la Ley Reguladora de las Haciendas Locales (TRLRHL), respectivamente por las DF 11ª y 12ª de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP).

<sup>4</sup> Según definición contenida en el artículo 24 de la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos

Las cuentas que recogen estos ingresos son:

De carácter financiero, cuentas de los siguientes subgrupos del PGCP

- 72. Impuestos directos y cotizaciones sociales
- 73. Impuestos indirectos
- 74. Tasas, precios públicos y contribuciones especiales

De carácter presupuestario

- Capítulo 1 de ingresos, impuestos directos
- Capítulo 2 de ingresos, impuestos indirectos
- Capítulo 3 de ingresos, tasas, precios públicos y otros ingresos

Hay que tener presente que las cuentas de ingresos tributarios están íntimamente relacionadas con las de deudores, de forma que la evidencia de auditoría que respalde las primeras también sirve para soportar las segundas y viceversa. En particular:

Deudores y acreedores, cuentas de los siguientes subgrupos del PGCP

- 43. Deudores presupuestarios
- 44. Deudores no presupuestarios
- 45. Deudores y acreedores por administración de recursos por cuenta de otros entes públicos
- 49. Deterioro de valor de créditos, y sus cuentas de cargo y abono:

Cuentas de pérdidas y ganancias

- 697. Pérdidas por deterioro de créditos
- 797. Reversión del deterioro de créditos

Cuando el alcance de una fiscalización esté limitado a la auditoría de los ingresos, aunque no se diga expresamente, se debe entender incluido en ese alcance la auditoría de las cuentas de activo relacionadas, sus saldos y movimientos de cargo y abono. Por esta razón la planificación y ejecución de la auditoría de estas áreas debe realizarse siempre de forma conjunta y coordinada.

#### 4. Objetivos de la auditoría del área

El **objetivo general de auditoría** del área consiste en determinar si los tributos han sido adecuadamente gestionados, liquidados y presentados en las cuentas anuales fiscalizadas, si estas reflejan de forma completa y exacta los ingresos del periodo, de acuerdo con las normas contables o presupuestarias aplicables, y si la gestión se ha realizado de conformidad con la normativa aplicable.

El auditor debe diseñar y aplicar procedimientos de auditoría que sean adecuados, teniendo en cuenta las circunstancias, de forma que le permita obtener evidencia de auditoría suficiente y adecuada para poder alcanzar conclusiones razonables en las que basar su opinión. (NIA-ES-SP 1500)

Se debe obtener evidencia suficiente y adecuada de que los ingresos del periodo contabilizados están libres de incorrección material, debida a fraude o error. Esto significa que las afirmaciones que subyacen en los tipos de transacciones, saldos contables e información a revelar (TTSCIR) son válidas. Las afirmaciones son el elemento central para la identificación y valoración de los riesgos inherentes, identificar los controles y para seleccionar los procedimientos de auditoría más eficaces.

## Guía práctica de fiscalización de los OCEX

### GPF-OCEX 1971 Guía de auditoría del área de ingresos por tributos

Las **afirmaciones** y los **objetivos detallados** de auditoría relacionados del área de **ingresos tributarios** son:

Afirmación		Descripción/Objetivo
Ocurrencia	O	Todos los ingresos tributarios contabilizados o revelados han ocurrido y dichas transacciones y hechos corresponden a la entidad.
Compleitud	C	Se han contabilizado todos los ingresos tributarios que tenían que registrarse y se ha incluido toda la información a revelar relacionada que se tenía que incluir en los estados financieros.
Exactitud	E	Las cantidades y otros datos relativos a los ingresos tributarios se han contabilizado adecuadamente y la correspondiente información a revelar ha sido adecuadamente medida y descrita.
Corte de operaciones	Co	Los ingresos tributarios se han contabilizado en el periodo correcto.
Clasificación	CI	Los ingresos tributarios se han contabilizado en las cuentas apropiadas.
Presentación	P	Los ingresos tributarios han sido adecuadamente agregados o desagregados y están descritos con claridad. La información a revelar es pertinente y comprensible en el contexto de los requerimientos del marco de información financiera aplicable.
Legalidad	L	Se ha cumplido la legalidad vigente en la gestión de los ingresos tributarios.

Las **afirmaciones** y los **objetivos detallados** de auditoría relacionados del área de **deudores** son:

Afirmación		Descripción/Objetivo
Existencia	E	Los deudores por ingresos tributarios pendientes de cobro existen.
Derechos y obligaciones	DO	El activo por deudores tributarios son derechos pendientes de cobro de la entidad.
Compleitud	C	Se han contabilizado todos los saldos de deudores pendientes de cobro que debían registrarse y se ha incluido toda la información a revelar relacionada que se tenía que incluir en los estados financieros.
Exactitud, valoración e imputación	E	Los derechos figuran en los estados financieros por los importes adecuados y las provisiones por morosos/incobrables son adecuadas. La correspondiente información a revelar ha sido adecuadamente medida y descrita.
Clasificación	CI	Los derechos pendientes de cobro se han contabilizado en las cuentas apropiadas.
Presentación	P	Los derechos pendientes de cobro han sido adecuadamente agregados o desagregados y están descritos con claridad y la correspondiente información a revelar es pertinente y comprensible en el contexto de los requerimientos del marco de información financiera aplicable.

Desde el punto de vista del control interno, con carácter general, verificaremos si los procedimientos administrativos y las normas de control interno definidos por la dirección son adecuados para asegurar un control efectivo y si han funcionado adecuadamente en el periodo auditado.

La **conclusión global de auditoría** del área debe ser inequívoca y debe expresar la opinión profesional (basada en la evidencia suficiente y adecuada obtenida tras todas las pruebas de auditoría realizadas) sobre si la cifra de ingresos tributarios y otras revelaciones relacionadas que reflejan las cuentas anuales es completa, exacta, está adecuadamente contabilizada y si la gestión ha sido conforme con la normativa.

#### 5. Obtención de conocimiento del proceso de gestión tributaria y de la aplicación TI que lo soporta

Para poder diseñar pruebas de auditoría eficaces, que permitan alcanzar el objetivo pretendido al auditar los ingresos tributarios, es necesario conocer los procedimientos de gestión que tenga implantados la entidad fiscalizada. No se puede auditar algo cuyo funcionamiento se desconoce.

De acuerdo con el apartado 25 de la GPF-OCEX 1315R (ver también el apartado 4 y 6 de la GPF-OCEX 5340) el auditor debe obtener conocimiento del sistema de información y comunicación de la entidad que sea relevante para la preparación de los estados financieros y para la gestión y contabilización de los ingresos tributarios en este caso.

Para ello, debe aplicar procedimientos de valoración del riesgo a través del conocimiento de las actividades de procesamiento de la información de la entidad, incluidos sus datos e información, los recursos que se deben utilizar en esas actividades de gestión de los ingresos tributarios, y obtener conocimiento sobre:

(a) el modo en que la información fluye por el sistema de información de la entidad, incluido el modo en que:

- las transacciones se inician y la información que sobre ellas se registra, se procesa, se corrige si es necesario, se traslada al mayor y se incluye en los estados financieros; y
- la información sobre los hechos y condiciones, distintos de las transacciones, que se captura, se procesa y se revela en los estados financieros;

(b) los registros contables, cuentas específicas de los estados financieros y otros registros de soporte relacionados con los flujos de información en el sistema de información;

(c) el proceso de información financiera utilizado para la preparación de los estados financieros de la entidad, incluida la información a revelar; y

(d) los recursos de la entidad, incluido el entorno de TI, relevantes para los apartados (a) a (c) anteriores, (la aplicación informática que soporta el proceso de gestión de ingresos tributarios y las interfaces existentes, entre otras cuestiones).

#### **Memorándum/narrativa**

Aunque en cada entidad habrá ligeras variaciones, básicamente interesa conocer y documentar el proceso de gestión de los tributos, desde el nacimiento de la obligación tributaria hasta su pago, así como la gestión de las posibles devoluciones de ingresos indebidos y la contabilización de esas transacciones.

Para ello, se debe entrevistar a las personas responsables de las distintas tareas, elaborar una narrativa descriptiva y realizar pruebas paso a paso (ver GPF-OCEX 1511) para confirmar que el conocimiento de los procedimientos aplicados es correcto, es decir, que la descripción se corresponde con los procedimientos ejecutados en la práctica por la entidad. Debe documentarse de forma clara para facilitar la identificación de riesgos que afecten a las cuentas anuales o al cumplimiento de la legalidad y así poder centrar las pruebas de auditoría en esos riesgos.

Para facilitar la adquisición del conocimiento de los procedimientos de gestión y su documentación se puede utilizar el formulario modelo que se adjunta en el Anexo 1, pero también pueden utilizarse narrativas o memorándums alternativos a ese modelo que sean lo suficientemente claros y descriptivos.

Si la entidad dispone de **procedimientos formalizados por escrito**, la narrativa a realizar por el auditor será tanto más breve cuanto más completos y claros sean aquéllos, que serán archivados completos en el Archivo Permanente de los papeles de trabajo electrónicos y un resumen (tan extenso como se considere necesario) también en el Archivo Corriente, y serán adecuadamente referenciados. Por esta razón, **dichos procedimientos deberán solicitarse al principio de la auditoría.**

#### **Descripción gráfica del proceso de gestión de los ingresos tributarios**

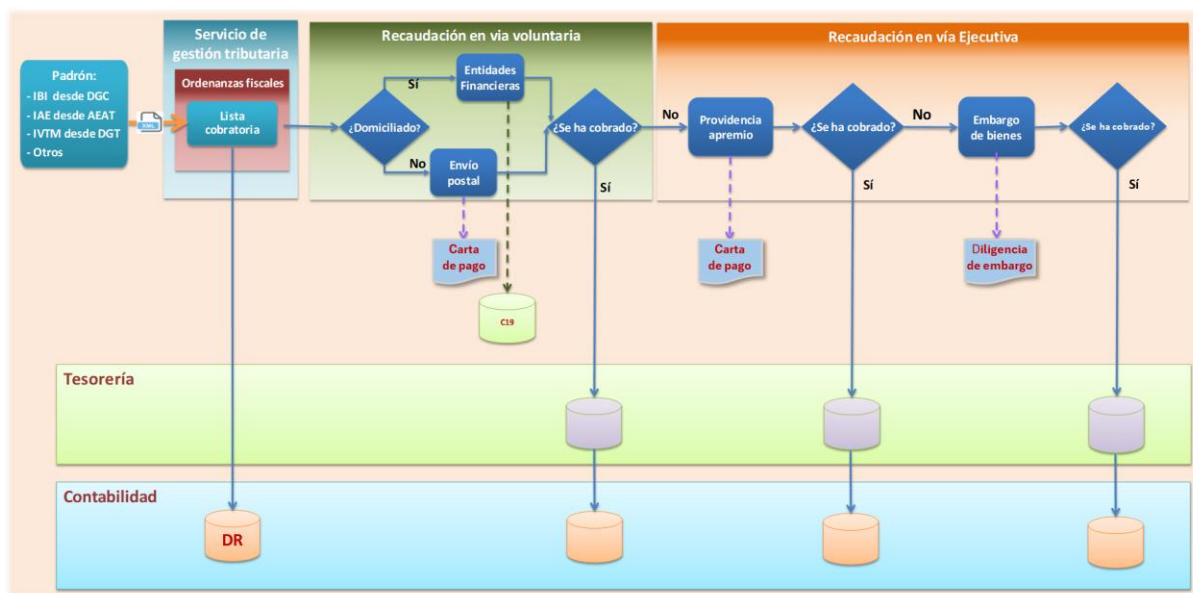
Es necesario complementar la narrativa con diagramas de flujo y tablas de riesgos y controles. Cuando se trata de procesos de gestión complejos como el que estamos estudiando, se empezará dibujando el mapa del proceso o flujograma general (como el del ejemplo siguiente), señalando los principales subprocesos o funciones, que posteriormente se han de describir con mayor detalle, y los departamentos implicados en cada uno de ellos. (Ver GPF-OCEX 1512).

En una entidad de tamaño mediano o grande, el proceso de gestión tributaria está soportado por una aplicación informática, que puede estar integrada o interrelacionándose con otras. Habrá que tener especial cuidado al analizar las interfaces que relacionan la aplicación con el resto de las aplicaciones de gestión, en especial con la contable y la de tesorería.

Para identificar y analizar las aplicaciones de gestión y las interfaces existentes (fundamentalmente con contabilidad y con tesorería) será conveniente contar con la colaboración de expertos en auditoría de sistemas de información. Se documentará detalladamente cada una de las principales aplicaciones utilizadas por la entidad para la gestión tributaria, la contabilización y el cobro, así como las interfaces existentes entre ellas.

Se incorpora, a continuación, y a modo de ejemplo, la descripción gráfica de lo que podría ser el sistema de gestión tributaria de un impuesto de entidad local gestionado bajo la fórmula de contraído previo.

En el supuesto de un tributo en el que su normativa haya establecido el sistema de contraído simultáneo al cobro (autoliquidación) la única modificación en el esquema anterior se basa en la inexistencia de un listado cobratorio que se contrae (aprueba) con anterioridad al proceso de recaudación, por lo que el servicio de gestión e inspección tributaria deberá haber implementado un proceso regular de comprobación y cotejo de hechos imponibles acaecidos y autoliquidaciones ingresadas.



## 6. Identificación de los riesgos de incorrección material (RIM) (Ver apartado 4.2 y 5 de la GPF-OCEX 5340)

### 6.1 Identificación y valoración de los RIM en los estados financieros (Ver apartado 5.1 de la GPF-OCEX 5340)

Se deberán identificar y valorar los RIM en los estados financieros y/o el área de gestión tributaria con la finalidad de (a) determinar si dichos riesgos **afectan a la valoración de riesgos en las afirmaciones** y (b) evaluar la naturaleza y extensión de su **efecto generalizado** sobre los estados financieros.

Los RIM en los estados financieros se refieren a los riesgos que se relacionan de forma generalizada con los estados financieros en su conjunto o con el área de gestión tributaria en particular, pero que pueden afectar a muchas afirmaciones (por ejemplo, (a) si la entidad tiene una administración tributaria desorganizada afectará de forma generalizada a los componentes de los estados financieros auditados y, en especial, si el entorno de control es deficiente; otro ejemplo sería (b) si la entidad tiene establecido un sistema de gestión tributaria totalmente automatizado con muy poca intervención humana, pueden esperarse riesgos derivados del uso de las TI incluyendo ciberriesgos).

Si los riesgos identificados tienen un efecto generalizado en los estados financieros requerirán una respuesta global de acuerdo con la NIA-ES-SP 1330. Una posible respuesta a (a) sería incrementar las pruebas sustantivas, y a (b) planificar la intervención de un equipo de auditoría de sistemas de información. Estos riesgos también pueden afectar a las afirmaciones individuales y, por lo tanto, también pueden ayudar a determinar los procedimientos posteriores de auditoría para abordar los riesgos identificados en las afirmaciones.

La identificación de los riesgos en los estados financieros y/o el área de gestión tributaria se ve influenciada por:

- (a) El conocimiento por parte del auditor del sistema de control interno de la entidad, en particular la evaluación e identificación de deficiencias en los controles indirectos (CGTI).
- (b) Susceptibilidad a la incorrección debido a factores de riesgo de fraude que afectan al riesgo inherente (el riesgo de fraude en el área de gestión tributaria es muy importante).

#### 6.2 Identificación y valoración de los riesgos inherentes en las afirmaciones

Al analizar el proceso de gestión se deben identificar, en cada una de sus fases, los riesgos inherentes existentes en las afirmaciones, valorarlos, elaborar el espectro de riesgo inherente y determinar aquellos riesgos que se considerarán significativos (los que se encuentran próximos al límite superior del espectro de riesgo inherente).

Cuando se aborda el análisis de los riesgos de un determinado proceso de gestión el enfoque principal consiste en responder, tanto con carácter general, como en cada una de las fases del proceso analizado, a la pregunta:

**¿Qué puede ir mal en el proceso de gestión tributaria que pueda afectar significativamente a las cuentas anuales o al cumplimiento de la legalidad?**

También se puede formular la pregunta así:

¿Qué podría ocurrir en esta fase que pudiera afectar negativamente en la consecución de los objetivos del proceso?

¿Representaría esto un RIM?

Se deben repetir estas preguntas en cada una de las etapas del proceso, teniendo en cuentas los factores de riesgo inherente.

La identificación de los riesgos potenciales se realiza entrevistando a usuarios y responsables del proceso de gestión auditado y analizando los distintos pasos y componentes que intervienen en el proceso (ver Anexo 1):

- El flujo de procesamiento de los datos
- Los permisos o autorizaciones
- Las interfaces (datos entrantes y salientes)
- Los datos maestros
- La segregación de funciones

Para facilitar el trabajo se pueden establecer listas previas sistematizadas y ordenadas, como la de la siguiente Tabla 1, en la que se señalan algunos de los principales riesgos inherentes que pueden existir.

Al completar la tabla siguiente, en la columna magnitud se pondrá el importe estimado de la incorrección potencial esperada. Dado que solo se deben tener en cuenta los riesgos materiales, se descartarán aquellos riesgos inherentes cuya magnitud no se acerque al nivel de materialidad que previamente hayamos definido de acuerdo con las NIA-ES-SP 1320 y GPF-OCEX 1321 (2024) para cada TTSCIR. Por ejemplo, se pueden descartar aquellos riesgos cuyo efecto estimado sea inferior a la cifra de incorrecciones claramente insignificantes (**ICI-TSI**), definida en la nueva GPF-OCEX 1321 (2024) para cada TTSCIR.

Se debe realizar o discutir este análisis en una reunión del equipo (ver GPF-OCEX 1513).

Valorar el riesgo inherente sin tener en cuenta los controles de la entidad, ayuda a evitar, por ejemplo, realizar valoraciones de riesgo inherente inadecuadamente bajas basadas en supuestos o en la **confianza excesiva** de que los controles funcionan de manera eficaz, sin haber evaluado el diseño y probado la eficacia operativa de dichos controles.

La siguiente tabla es un ejemplo orientativo, no es exhaustiva.

## Guía práctica de fiscalización de los OCEX

### GPF-OCEX 1971 Guía de auditoría del área de ingresos por tributos

**Tabla 1. Ejemplo de valoración de los riesgos inherentes en las afirmaciones**

#	Riesgos inherentes	Función	Afirmación	Probabilidad (1 a 10)	Magnitud (1 a 10)	Valoración del R.I. (PxM)
RI01	Errores en la importación o transmisión de los datos facilitados por otras entidades (Catastro, DGT, etc.) Manipulación de los datos de origen.	Elaboración del Padrón	E, C, L			
RI02	No se identifican todos los hechos impositivos que dan lugar a una obligación tributaria.	Autoliquidaciones o liquidaciones	E, C, L			
RI03	Las autoliquidaciones presentadas no se revisan y, por ello, no se subsanan los incumplimientos de la normativa tributaria por parte del contribuyente.	Autoliquidaciones	E, L			
RI04	Inadecuada aplicación de tipos impositivos, exenciones, beneficios fiscales, etc.	Elaboración de las listas cobratorias o liquidaciones tributarias	E, L			
RI05	Las liquidaciones no se aprueban o son aprobadas por personas que carecen de la competencia para ello.	Aprobación de las listas cobratorias y liquidaciones	L			
RI06	Las notificaciones no se realizan en tiempo y forma adecuadas, lo que puede dar lugar a la prescripción de la deuda.	Notificaciones	O, DO, L			
RI07	Los aplazamientos y fraccionamientos no se aprueban de acuerdo con los requisitos fijados en la normativa y se aprueban por las personas sin competencia para ello.	Aplazamientos y fraccionamientos	L			
RI08	Debilidades en el proceso de gestión dan lugar a la caducidad de los procedimientos y la prescripción del derecho de la Administración a liquidar.	Gestión tributaria	C, DO, L			
RI09	No se dictan las providencias de apremio de todas aquellas deudas no satisfechas en el periodo voluntario. La expedición de las providencias de apremio se retrasa injustificadamente. Las providencias de apremio no se dictan por los órganos con competencia para ello.	Expedición de providencias de apremio	C Co L			
RI10	Se tarda en iniciar el procedimiento recaudatorio de apremio o no se tramita con los recargos correspondientes desde la fecha de fin del plazo de voluntaria	Aplicación de los recargos de ejecutiva	L, E Co			
RI11	Pueden realizarse reposiciones de recibos y liquidaciones a voluntaria que no cumplen los requisitos legales.	Reposición a voluntaria	L			
RI12	Se pueden realizar anulaciones de liquidaciones de ingresos que no cumplen con los requisitos legales y/o no se autorizan por los órganos con competencias para ello.	Bajas de liquidaciones en voluntaria o en ejecutiva	C, L			
RI13	El contribuyente no realiza efectivamente el ingreso del tributo o retrocede el movimiento de ingreso tras la presentación del justificante de pago, pero se registra un ingreso.	Recaudación				
RI14	Los cobros en voluntaria y ejecutiva no se controlan ni registran contablemente de forma adecuada.	Recaudación	C, L			
RI15	Se realizan devoluciones de ingresos tributarios que no cumplen la normativa vigente.	Devolución de ingresos indebidos	C, L			
RI16	Se producen retrasos en la gestión de solicitudes de devolución de ingresos indebidos, lo que provoca un coste para la Administración por intereses de demora.	Devolución de ingresos indebidos	Co, L			



#	Riesgos inherentes	Función	Afirmación	Probabilidad (1 a 10)	Magnitud (1 a 10)	Valoración del R.I. (PxM)
RI17	Los datos maestros (clasificación de tributos, tipos impositivos, periodos de voluntaria, periodos de ejecutiva, porcentaje de los recargos en ejecutiva, etc.) no son completos y exactos.	Mantenimiento de datos maestros	E, L			
RI18	Se contabilizan de forma incorrecta los ingresos correspondientes a las liquidaciones y autoliquidaciones. Existen liquidaciones aprobadas y notificadas que no se han registrado contablemente o se han dado de baja indebidamente. También se podrían modificar indebidamente liquidaciones de tributos correctamente aprobadas y contabilizadas.	Contabilidad	CI, P			

### 6.3 Determinar los riesgos significativos en el espectro de riesgo inherente (Ver apartado 5.6 de la GPF-OCEX 5340)

Una vez completada una tabla como la Tabla 1, una forma fácil de calcular el espectro de riesgo inherente consistirá en ordenarla según el valor, de mayor a menor, de la columna “Valoración del R.I.”.

Serán **riesgos significativos** los que estén ubicados en la parte alta de la tabla. El límite para distinguir cuales son riesgos significativos y cuáles no, será una cuestión de juicio profesional y dependerá de las circunstancias.

### 6.4 Determinar los riesgos para los que los procedimientos sustantivos por sí solos no proporcionan evidencia de auditoría suficiente y adecuada (Ver apartado 5.7 de la GPF-OCEX 5340)

El auditor también debe determinar qué riesgos no pueden ser abordados únicamente con procedimientos sustantivos, que no pueden proporcionar evidencia de auditoría suficiente y adecuada con respecto a alguno de esos riesgos significativos en las afirmaciones y, por tanto, se requiere la aplicación de pruebas de controles.

Este puede ser el caso en aquellas circunstancias en las que una cantidad significativa de la información de la entidad se inicia, registra, procesa o notifica solo de manera electrónica, como en un ERP que implica un alto grado de integración a través de sus aplicaciones de TI. Un ejemplo claro de esto sería la auditoría de una entidad mediana o grande, en la que el proceso de gestión tributaria está **muy automatizado** con escasa o nula intervención manual y **la evidencia de auditoría únicamente está disponible en formato electrónico** y su suficiencia y adecuación dependen de la eficacia de los controles sobre su exactitud y completitud.

*Por ejemplo: al auditar el IBI de un gran ayuntamiento, con cientos de miles de transacciones automatizadas, probablemente basarse únicamente en procedimientos sustantivos no permitirá reducir el riesgo de auditoría a un nivel aceptable y será preciso valorar el riesgo de control y revisar los CPI y los CGTI relacionados.*

La posibilidad de que la información se inicie o altere de manera incorrecta y de que este hecho no se detecte puede ser mayor si los correspondientes controles no están funcionando de manera eficaz. En estas circunstancias, la única forma de obtener evidencia de auditoría suficiente y adecuada es comprobar la eficacia operativa de los controles existentes.

Un aspecto relevante a considerar es la posible existencia de procedimientos administrativos automatizados en los que no interviene un funcionario persona física en la tramitación y resolución del procedimiento. En estos casos, si las transacciones son significativas y se han valorado con un nivel elevado de riesgo inherente se deberá verificar si se han cumplido todos los requisitos y aprobaciones en el establecimiento del procedimiento automatizado y que los controles implantados funcionan correctamente.

### 6.5 Los riesgos de fraude en el área de gestión tributaria

El área de ingresos tributarios ha sido tradicionalmente un área susceptible a riesgos de fraude:

- Omisión o falseamiento de los hechos imponible por parte del contribuyente.
- Sustracción de efectivo cobrado de liquidaciones tributarias.
- Manipulación indebida de liquidaciones por un agente interno para reducir la carga fiscal de determinado/s contribuyente/s.
- Accesos al sistema por agentes externos, aprovechando la debilidad de los controles de acceso, para manipular los datos de deudas tributarias.

- Concesión indebida o no autorizada de aplazamientos, bonificaciones o exenciones, mediante un agente interno o un acceso no autorizado al sistema aprovechando su debilidad.
- Manipulación de los datos al transmitirlos con las interfaces.

Para minimizar el fraude se debe:

- Establecer los procedimientos de gestión y asignación de responsabilidades claras y por escrito.
- Establecer un sólido sistema de control interno, incluido una adecuada segregación de funciones.
- Implantar unos controles de acceso a los sistemas y a las bases de datos sólidos y eficaces, ya que de su buen funcionamiento dependerán los dos primeros.
- Revisar las verificaciones efectuadas por las auditorías internas.

El auditor deberá incluir en sus procedimientos de auditoría la revisión de estos aspectos. En un entorno de administración electrónica avanzado cualquier sistema de control interno debe incluir un sólido sistema de ciberdefensa basado en el ENS, es decir, **los CPI deben estar respaldados por los CGTI necesarios ya que si no cualquier sistema de control interno carecerá de fiabilidad**. Para su revisión se deberá contar con la ayuda de especialistas en auditoría de sistemas, que también revisarán la integridad de las interfaces.

## 7. Identificación de los controles de procesamiento de la información (CPI) relevantes

### 7.1 Qué son los CPI relevantes

Tras la narrativa, el dibujo de los flujogramas y la identificación de los riesgos y controles existentes, estos se recogerán en unas tablas que relacionen los riesgos significativos identificados (los que están en la parte superior del espectro de riesgo inherente tal como se ha visto antes) con los CPI. Un ejemplo posible es la Tabla 2 siguiente.

Además de identificar los riesgos inherentes del proceso de gestión, en las interfaces y en los datos maestros, debe adquirirse una comprensión preliminar de los CPI (manuales o automatizados) que mitiguen dichos riesgos.

En esta fase, el auditor identificará los **CPI**, que son controles aplicados durante el procesamiento de la información en el sistema de información de la entidad y **responden directamente a los riesgos para la integridad de la información, es decir, la completitud, exactitud y validez de las transacciones y otra información**<sup>5</sup>. A estos objetivos, en el sector público hay que añadir el de **legalidad**.

Teniendo en cuenta la complejidad de los procesos y de las aplicaciones de gestión en los actuales entornos de gestión tributaria, es importante centrarse en lo esencial, por ello la identificación de los riesgos significativos y de los CPI implantados para mitigarlos constituye la base para una auditoría eficaz. Solo se revisarán aquellos CPI que tengan relevancia a efectos de la auditoría, circunstancia que deberá ser definida por el auditor a partir de los riesgos significativos identificados.

**Serán CPI relevantes** los controles que el auditor debe identificar, cuyo diseño debe evaluar y cuya implementación debe verificar. Según la GPF-OCEX 1315R (25 y A151) y la GPF-OCEX 5340 (apartado 5.7) son:

- **Controles que responden a riesgos que se consideran significativos.** El conocimiento obtenido acerca del enfoque de la dirección para responder a esos riesgos puede proporcionar una base para el diseño y aplicación de procedimientos sustantivos que respondan a riesgos significativos. Generalmente incluyen políticas, procedimientos, prácticas y una estructura organizativa que son esenciales para que la dirección pueda reducir los riesgos significativos y alcanzar el objetivo de control relacionado.
- Se requerirá el conocimiento de:
  - Espectro de riesgo inherente.
  - Controles que la entidad ha diseñado e implementado para los riesgos significativos derivados de cuestiones no rutinarias o que requieran la aplicación de juicio, como por ejemplo la revisión de hipótesis por la alta dirección o por expertos, documentación de las estimaciones contables o la aprobación por los responsables de la entidad.
  - Controles que la dirección ha diseñado, implementado y mantenido para prevenir y detectar el fraude.

---

<sup>5</sup> Apartado A148 de la NIA-ES 315R/GPF-OCEX 1315R.

- **Controles sobre asientos en el diario**, incluidos aquellos asientos que no son estándar y que se utilizan para registrar transacciones o ajustes no recurrentes o inusuales.

Generalmente, el modo en que una entidad incorpora información del procesamiento de transacciones en el mayor es mediante la utilización de asientos en el diario, tanto estándar como no, o automatizados o manuales. La identificación de asientos no estándar en el diario, en los sistemas de mayores manuales requerirá la inspección de los mayores, diarios y documentación soporte. Si se utilizan procesos automatizados para la llevanza de los libros, el uso de técnicas de auditoría automatizadas facilitará esta identificación.

- **Controles cuya eficacia operativa tiene previsto comprobar para determinar la naturaleza, el momento de realización y la extensión de los procedimientos sustantivos.**

La evaluación estos controles proporciona al auditor la base para el diseño de procedimientos de pruebas de controles de conformidad con la NIA-ES-SP 1330.

- **Controles que responden a riesgos para los cuales los procedimientos sustantivos por si solos no proporcionan evidencia de auditoría suficiente y adecuada.**

- **Otros controles** que el auditor considere adecuado identificar, como:
  - Controles que responden a riesgos valorados como más alto dentro del espectro de riesgo inherente pero que no han sido considerados riesgos significativos.
  - Controles relacionados con conciliaciones de registros detallados con el mayor.
  - En el caso de utilizar una organización de servicios, controles complementarios de la entidad usuaria. Si se utilizan servicios de computación en la nube se tendrá en consideración la GPF-OCEX 1403.

En la revisión de estos controles se analizará si respaldan más de un objetivo de control y si hacen frente directamente a los riesgos significativos. En su evaluación se tendrá también en cuenta que los controles preventivos son, por regla general, más eficientes que los detectivos y que los controles automatizados son más fiables que los controles manuales. Cuando múltiples controles alcancen individualmente el mismo objetivo, no es necesario identificar cada uno de los controles relacionados con dicho objetivo.

**Los controles que responden a los riesgos de incorrección material en las afirmaciones, individualmente o combinados entre ellos, son indispensables para la reducción de los riesgos a un nivel aceptable.** Son los que permiten reducir los riesgos de incorrección material (RIM) a un nivel aceptablemente bajo.

Los CPI relevantes constituyen el elemento fundamental del sistema de control y deben ser, pues, objeto de comprobación prioritaria; los otros controles tienen menos importancia para el auditor. **Todo el trabajo de auditoría posterior debe centrarse en estos controles, ya que todo trabajo que se realice sobre los otros controles existentes no aporta satisfacción o utilidad adicional de auditoría, y será un trabajo ineficiente.**

Para documentar la valoración del riesgo de control se puede cumplimentar una tabla como la siguiente relacionando riesgos inherentes significativos para las afirmaciones identificados con los CPI relevantes.

**Tabla 2. Riesgos inherentes significativos en las afirmaciones y CPI relevantes**

TTSCIR	Afirmación	Riesgos (inherentes) significativos	CPI relevantes
Para cada tipo de transacción	Occurrencia		
	Compleitud		
	Exactitud		
	Corte de operaciones		
	Clasificación		
	Presentación		
	Legalidad		

TTSCIR	Afirmación	Riesgos (inherentes) significativos	CPI relevantes
Para cada saldo contable	Existencia		
	Derechos y obligaciones		
	Compleitud		
	Exactitud, valoración e imputación		
	Clasificación		
	Presentación		

Si hay varios controles que tienen el mismo objetivo, el auditor deberá entender cada uno de ellos y seleccionar como controles relevantes aquellos que considere que alcanzan más eficazmente su objetivo y teniendo en cuenta el coste/eficacia que puede suponer su comprobación.

Se debe analizar si el equilibrio entre controles manuales/automatizados y entre preventivos/correctivos es adecuado. Una excesiva confianza en controles manuales en un entorno informatizado puede ser un indicador de debilidad del control interno.

El auditor debe evitar depositar un exceso de confianza en los controles automatizados en un entorno de administración electrónica mediante una adecuada revisión de su diseño, implantación y eficacia operativa.

## 7.2 Principales controles internos del área de ingresos tributarios

La entidad auditada debe mantener un exhaustivo control interno sobre todas las fases de la gestión tributaria ya que la falta de controles puede incentivar actividades fraudulentas o dejar de recaudar ingresos.

Los **principales controles** incluirán (relación no exhaustiva):

- Los **procedimientos** de gestión han de constar por escrito y reflejar los límites y autorizaciones.
- Existencia de una adecuada **segregación de funciones** en todo el proceso.
- **Controles de acceso:** Solo los funcionarios de gestión tributaria deben tener acceso a la aplicación de gestión y la **asignación de permisos** a los usuarios de esa aplicación se realizará aplicando el principio de mínimo privilegio.  
Los usuarios con acceso a la aplicación tributaria/recaudación se revisan periódicamente para garantizar que los privilegios estén restringidos al personal adecuado.
- Controles sobre la **elaboración del Padrón**
  - Controles para mantener la integridad de la información al importar los datos de origen, para elaborar el padrón, y también una vez almacenados en los sistemas de la entidad auditada.
  - Controles de acceso a la información en los sistemas de la entidad.
- Controles sobre el **mantenimiento de datos maestros**
  - Se dispone de controles que garantizan la exactitud y completitud de los datos maestros utilizados.
  - Hay una adecuada segregación de funciones.
- Controles sobre las **autoliquidaciones**
  - Se dispone de controles que permiten detectar todos los hechos imponible sujetos a tributación (por ejemplo, cruzando información procedente de notarías, registro civil, etc.) y se realizan liquidaciones para todos los casos en los que el obligado tributario no ha autoliquidado el impuesto correspondiente.
  - Las autoliquidaciones presentadas son revisadas de manera sistemática.
  - En los casos de incumplimiento de la normativa, se aprueba la liquidación y, si procede, la sanción

correspondiente según la normativa tributaria.

- Controles sobre la **elaboración de las listas cobratorias o liquidaciones tributarias**
  - En la elaboración de listas cobratorias y liquidaciones se realizan por las personas que tienen atribuidas las competencias, de acuerdo con la normativa aplicable.
  - Las listas cobratorias y liquidaciones se revisan por personas diferentes de las que las elaboran.
  - Se aplican los tipos impositivos, exenciones, beneficios fiscales aprobados y vigentes.
  - Los cálculos matemáticos son correctos y los datos maestros utilizados en los cálculos son exactos.
- Controles sobre las **notificaciones**
  - El proceso de notificación dispone de controles que aseguran el cumplimiento de los requisitos establecidos por la normativa.
  - Existen controles posteriores para el análisis de la eficacia del proceso de notificación.
- Controles sobre los **aplazamientos y fraccionamientos**
  - Los aplazamientos y fraccionamientos se gestionan de forma ágil y se aprueban por las personas autorizadas, respetando los criterios establecidos en la normativa.
- Controles sobre la **expedición de providencias de apremio**
  - Las providencias de apremio se realizan automáticamente cuando finaliza el periodo de voluntaria, sin retrasos y se aprueban por personas con competencia para ello.
- Controles sobre la aplicación de los **recargos de ejecutiva**
  - Los valores tributarios en ejecutiva se liquidan automáticamente con los recargos legales marcados por la normativa tributaria.
  - No existen retrasos en iniciar la fase ejecutiva.
- Controles sobre la **reposición a voluntaria**
  - La aprobación de reposición de liquidaciones a voluntaria se realiza de acuerdo con los requisitos legales y son aprobadas por el órgano que tiene legalmente atribuidas las competencias necesarias.
  - Las reposiciones a voluntaria se revisan por personas distintas a las que las aprueban.
- Controles sobre las **bajas de liquidaciones en voluntaria o en ejecutiva**
  - La anulación de liquidaciones se realiza de acuerdo con la normativa de aplicación y es aprobada por el órgano que dispone de las competencias necesarias.
  - Las bajas se revisan por personas distintas a las que las aprueban.
- Controles en **recaudación**
  - No se permite la retrocesión de los pagos realizados por el contribuyente (a excepción de las previsiones establecidas en la Ley de Servicios de Pago).
  - Existe un adecuado control de todos los ingresos en voluntaria y en ejecutiva y se registran contablemente en tiempo y de forma adecuada.
  - No se realizan ningún cobro por caja.
- Controles en **contabilidad**

Todos los ingresos tributarios se contabilizan de manera adecuada. Se dispone de controles que aseguran:

  - La contabilización de todos los ingresos, tanto en periodo voluntario como en ejecutiva, desde que nace el derecho a recaudar de la Administración.
  - La contabilización de las anulaciones de las liquidaciones y autoliquidaciones.
  - La contabilización de las devoluciones de ingresos.

- Revisión de las liquidaciones realizadas.
  - Conciliación periódica de saldos de deudores tributarios por personal independiente.
  - La segregación de funciones en las tareas de gestión tributaria.
  - Informe de revisión sobre los ingresos liquidados, bajas, cobrados y contabilizados.
  - Los tipos impositivos aplicados en las liquidaciones son los aprobados y vigentes (Fichero maestro de tipos impositivos).
  - Los periodos de recaudación en voluntaria son los recogidos en la normativa y son los vigentes para el periodo auditado. Segregación de funciones para la introducción y modificación de datos en las tablas de periodos de cobro de voluntaria. Informes de revisión de los periodos de recaudación.
  - Existen controles para garantizar la integridad de la interfaz entre la aplicación de ingresos y recaudación y la de contabilidad.
- Controles sobre **devoluciones de ingresos**
    - Las devoluciones tributarias se realizan según los criterios establecidos por la normativa vigente, son aprobadas por los órganos con competencia para ello y en ningún caso se realizan devoluciones de ingresos que previamente no han sido satisfechos.
    - Las solicitudes de ingresos indebidos se gestionan en tiempo y forma, evitando retrasos innecesarios que den lugar al aumento de los intereses de demora a pagar por la Administración.
  - En un entorno de administración electrónica avanzada, el establecimiento **de unos sólidos CGTI para garantizar estos CPI es absolutamente crítico**, ya que la mayor parte de los CPI anteriores son dependientes del buen funcionamiento de los CGTI.

## 8. Evaluación del diseño e implementación (D+I) de los CPI relevantes

Para cada uno de los controles (CPI+CGTI) identificados como **relevantes** el auditor debe:

- a) **Evaluar si el control está diseñado (D) eficazmente** para responder al RIM en las afirmaciones (CPI) o si está diseñado eficazmente para sustentar el funcionamiento de otros controles (CGTI). Implica que el auditor considere si el control, de manera individual o en combinación con otros controles, es capaz de prevenir de modo eficaz, o de detectar y corregir, incorrecciones materiales (es decir, permite alcanzar el objetivo de control) o si es capaz de sustentar el funcionamiento de otros controles.
- b) **Determinar si el control ha sido implementado (I)** estableciendo que el control existe y que la entidad lo está utilizando.

Para cada CPI que se identifique como relevante, el auditor debe aplicar procedimientos de valoración del riesgo (PVR) para **analizar la efectividad de su diseño para realizar la actividad de control y su implementación**, considerando el riesgo TI y los objetivos de la auditoría. Si se concluye que el diseño e implementación es eficaz se aplicarán procedimientos posteriores de auditoría para **verificar, mediante una prueba de control, si está en funcionamiento durante todo el periodo auditado**.

Para más información, ver el apartado 8 de la GPF-OCEX 5340.

## 9. Valoración del riesgo de control

Si bien el auditor siempre está obligado a valorar el riesgo inherente de los riesgos identificados a nivel de afirmación, **solo se exige valorar el riesgo de control si se tiene previsto probar la eficacia operativa de los controles o cuando los procedimientos sustantivos por sí solos no proporcionan suficiente evidencia de auditoría a nivel de afirmación**.

Si el auditor no tiene previsto comprobar la eficacia operativa de los controles, su valoración del RIM será la misma que la valoración del riesgo inherente. En estos casos, en los que se tiene previsto adoptar un enfoque fundamentalmente sustantivo de la auditoría, una vez que se haya obtenido el conocimiento de los componentes del sistema de control interno que se exige en los apartados 21 a 27 de la NIA-ES 315R/GPF-OCEX 1315R, no será necesario realizar procedimientos adicionales.

Existe un vínculo estrecho entre el trabajo realizado para obtener un conocimiento de los componentes del sistema de control interno de la entidad, su D+I, y la valoración del riesgo de control. El conocimiento por parte del auditor del sistema de control interno de la entidad informa sus expectativas sobre la eficacia operativa de los controles y si el auditor planea probar la eficacia operativa de los controles, ese conocimiento le ayudará en el diseño y la realización de procedimientos de auditoría posteriores de acuerdo con la NIA-ES-SP 1330.

Cualquier plan para probar la eficacia operativa de los controles se basa en la expectativa de que los controles funcionan eficazmente, y esto será la base de la valoración del riesgo de control por el auditor.

Para más información, ver el apartado 9 de la GPF-OCEX 5340.

#### 10. Revisión y evaluación de los CGTI: Factores de riesgo a considerar

La eficacia de los CPI automatizados depende en gran medida del buen funcionamiento de los controles generales de tecnologías de la información (CGTI). Por tanto, **la revisión de los CPI y la decisión de depositar confianza en ellos debe hacerse tras una evaluación previa de los CGTI**, según los procedimientos descritos en el apartado 10 de la GPF-OCEX 5340 y en la GPF-OCEX 5330.

El equipo de expertos en auditoría de sistemas de información al realizar la revisión de los CGTI deberá tener presente la GPF-OCEX 5330. A modo de ejemplo, se indican los siguientes riesgos derivados de la utilización de las TI, que están entre los más habituales en relación con la gestión tributaria.

##### **Entorno de control**

Un entorno de control efectivo es fundamental para asegurar que la información sobre los ingresos y el tratamiento de la información relacionada sean exactos y completos, y que se mantenga la integridad y confidencialidad de la información.

Ejemplo:

Deficiencia de control observada	Riesgo	Recomendación
<p>Durante la realización de la fiscalización se ha observado una serie de incumplimientos en los procedimientos de gestión y de control interno que ponen en cuestión la eficacia del sistema de control interno de la entidad y afectan a la fiabilidad de la información económico-financiera recogida en las cuentas anuales.</p> <p>Un elemento esencial en cualquier sistema de control interno es el denominado tono directivo. La forma en que la alta dirección expresa sus convicciones respecto de la importancia del control interno y determina en gran medida su eficacia.</p>	<p><b>Alto</b></p> <p>Debido a las circunstancias indicadas no se puede tener la seguridad de que todos tributos se hayan tramitado de acuerdo con los procedimientos aprobados, hayan tenido entrada en el sistema administrativo contable y estén adecuadamente recogidos en las cuentas anuales.</p>	<p>Recomendamos que los órganos de dirección establezcan, formalicen, comuniquen, mantengan operativos y exijan su cumplimiento, los procedimientos administrativos de gestión que requiera la actividad de la entidad y un sistema de control interno que garanticen el cumplimiento de los principios de buena administración.</p>

##### **Gestión de cambios**

Es importante que existan unos controles efectivos a fin de asegurar que los cambios en las aplicaciones sean autorizados y debidamente comprobados antes de introducirlos en el sistema de producción.

El procedimiento de gestión de cambios tiene como finalidad evitar que se introduzcan cambios en la programación sin la autorización apropiada, que pudiera posibilitar posteriormente modificaciones no autorizadas en la información sobre las autoliquidaciones y liquidaciones, las resoluciones dictadas por el órgano competente, o en la aplicación de gestión tributaria, etc. Contemplará entre otras cuestiones que:

- Todas las solicitudes de cambios a introducir en las aplicaciones de gestión tributaria, así como cualquier cambio en la estructura de la base de datos deberán ser revisados y aprobados por el responsable funcional antes de ser implementados.
- Todos los cambios deben probarse y autorizarse antes de ser introducidos en el entorno de producción.
- Debe existir separación de funciones a fin de limitar la capacidad del personal para realizar cambios que afecten tanto a la base de datos de producción como a la configuración de la aplicación de gestión tributaria.

Si una aplicación se ha desarrollado en la entidad y un equipo de desarrolladores internos tiene acceso a modificar la aplicación, el riesgo será alto, por lo que deben establecerse controles internos como la segregación de funciones y controles de supervisión.

Sin embargo, en una aplicación comercial cualquier cambio en el código fuente necesitará la intervención del fabricante y unos procedimientos adicionales.

Debido a la criticidad del sistema informático de gestión tributaria y a los aspectos fundamentales de sus operaciones, el mantenimiento y las actualizaciones de las aplicaciones deben ser incorporados a los procedimientos de gestión de cambios.

Ejemplo:

Deficiencia de control observada	Riesgo	Recomendación
Se han identificado debilidades en la asignación de la responsabilidad que otorga máximo nivel de privilegios en la aplicación de gestión tributaria. En concreto, se han identificado un total de 48 usuarios, de los que la mayoría corresponden a personal que realiza labores de desarrollo, con acceso a la aplicación y datos de producción. El acceso a producción para labores de desarrollo no debe permitirse, y menos aún, realizarse de forma generalizada.	<b>Alto</b> El personal con capacidades de desarrollo podría introducir modificaciones no autorizadas a los datos y programas que están en el entorno de producción, ya sea de forma accidental o deliberada, representando un riesgo alto de incorrecciones materiales significativas en las cuentas anuales .	Recomendamos que se implante un entorno de pruebas, aislado del de producción, que permita realizar de forma adecuada las labores de desarrollo, evitando de esta forma los accesos innecesarios a producción.

#### **Controles de acceso y gestión de usuarios**

Los riesgos en esta área están asociados con accesos indebidos a los sistemas, a los datos y a la información financiera o contable.

Una gestión eficaz de los controles de acceso de los usuarios proporciona garantía, mediante la aplicación del principio de mínimo privilegio, de que las aplicaciones de gestión tributaria, contabilidad y tesorería están adecuadamente protegidas para evitar el uso no autorizado, divulgación, modificación o pérdida de información o de fondos. La gestión de usuarios es un componente crítico para el establecimiento de una efectiva segregación de funciones.

Los parámetros críticos que pueden incidir en los accesos a las aplicaciones y bases de datos son:

#### *Número de usuarios activos*

El número de usuarios con acceso a una aplicación tiene un impacto directo en el riesgo de accesos o de transacciones no autorizadas (cuantos más usuarios mayor riesgo). Una aplicación con tres usuarios será considerada probablemente de bajo riesgo en este aspecto, sin embargo, una aplicación con 5.000 usuarios tendrá un nivel alto de riesgo porque existirán más probabilidades de errores humanos al conceder accesos y privilegios, de que existan accesos que presenten conflictos frente a lo que se considera una adecuada segregación de funciones o por una monitorización inadecuada de los accesos.

#### *Privilegios*

El acceso o la modificación de los privilegios de acceso deben ser aprobados y documentados, bajo el principio de mínimo privilegio y de necesidad de saber.

El acceso al sistema se basará en una estructura de roles de usuario.

#### *Número de administradores*

Como ocurre con el número de usuarios, el número de administradores de la aplicación tiene un impacto directo y proporcional con la valoración del riesgo. El acceso de administrador o acceso "privilegiado" debe estar limitado estrictamente a las necesidades de la entidad.

#### *Acceso directo a la Base de Datos (BD) subyacente*

Este es otro parámetro crítico, ya que puede dejar puertas traseras para acceder directamente a la BD sin necesidad utilizar la aplicación.

#### *Autenticación*

Los usuarios del sistema de gestión tributaria deberán ser identificados de forma única. Los usuarios tendrán un identificador individual de acceso y no deberán compartir contraseñas. Es muy importante



## Guía práctica de fiscalización de los OCEX

### GPF-OCEX 1971 Guía de auditoría del área de ingresos por tributos

evaluar los mecanismos de autenticación implantados en una aplicación de gestión para determinar la lista de personas con acceso a la misma.

Veamos algunos ejemplos:

Deficiencia de control observada	Riesgo	Recomendación
<p>Hemos observado que las directivas de contraseñas no son todo lo robustas que sería conveniente de acuerdo con las mejores prácticas en la materia. La deficiencia de control, que afecta a todos los niveles del sistema de información (SAP, Oracle, HP-UX, Directorio activo), nos ha permitido constatar intervalos de caducidad elevados, desbloqueo automático de cuenta en caso de superar los intentos de acceso fallido prefijados, periodo de tiempo elevado en el cierre de sesión por inactividad, no activación de requerimientos de complejidad de las contraseñas, elevado número de usuarios cuya contraseña no caduca, así como usuarios que no requieren de contraseña para acceder al sistema.</p>	<p><b>Alto</b></p> <p>Las deficiencias detectadas debilitan la efectividad del control de acceso en los distintos niveles de los sistemas de información representando un riesgo sobre la integridad y confidencialidad de los datos de la Entidad.</p>	<p>Implementar una política de contraseñas robustas, de acuerdo con las mejores prácticas en esta materia y adaptarlas a los parámetros generalmente aceptados (complejidad mínima, cambio de contraseñas cada 3 a 6 meses, historial de contraseñas mínimo de 5, bloqueos ante intentos fallidos, etc.) en todos los niveles del sistema de información de la Entidad (SAP, Oracle, HP-UX, Directorio activo).</p>
<p>Se han identificado 24 cuentas de usuario genéricas (lo que supone un 20,9% sobre el total de cuentas de usuario activas) cuyo uso no está justificado o bien no se conoce quién y para qué se utilizan.</p>	<p><b>Alto</b></p> <p>La utilización de cuentas genéricas impide mantener la trazabilidad de las acciones realizadas.</p>	<p>Realizar una revisión detallada de los usuarios existentes en la aplicación de gestión tributaria, con el fin de identificar las cuentas genéricas y conocer su uso. Estas cuentas deben ser sustituidas por cuentas nominativas, que permitan identificar al usuario responsable de las acciones realizadas con ellas.</p>
<p>No existe un procedimiento para las altas, bajas y modificaciones de los usuarios y sus permisos en las aplicaciones ni para la revisión periódica de dichos permisos. Existen usuarios que llevan inactivos varios meses o que no han accedido nunca.</p>	<p><b>Medio</b></p> <p>Esta situación implica un riesgo medio de accesos indebidos y de actuaciones no autorizadas.</p>	<p>Formalizar un procedimiento de gestión de usuarios y de permisos, que contemple los procesos y la implicación de los responsables de los diferentes departamentos en las altas, en los cambios de puesto de trabajo y en las bajas de los usuarios de dominio y de las aplicaciones.</p> <p>También debe incluir la realización periódica de revisiones de los usuarios autorizados y los permisos asignados en los sistemas y aplicaciones, de forma que se garantice que cada usuario dispone de las capacidades mínimas necesarias para desempeñar sus tareas y ninguna más. Debe conservarse la documentación acreditativa de las revisiones realizadas, los resultados y las acciones llevadas a cabo.</p>
<p>El acceso a la aplicación utilizada para administrar aspectos críticos de la aplicación tributaria (parámetros de configuración, usuarios, etc.) no se encuentra adecuadamente limitado.</p> <p>Hemos identificado accesos concedidos a cuentas genéricas, a personal de desarrollo, a personal que ha sido baja, etc.</p> <p>Por otro lado, esta aplicación de administración no permite definir roles y hacer una adecuada asignación de privilegios, lo que conlleva que personal que requiere acceder a la aplicación para realizar determinadas funciones disponga también de la opción de administrar usuarios y privilegios, capacidad que debe estar restringida únicamente al personal autorizado para ello.</p>	<p><b>Alto</b></p> <p>Los privilegios relacionados con la administración de usuarios deben estar adecuadamente restringidos, respondiendo siempre al principio de mínimo privilegio.</p> <p>Debilidades en el control sobre los usuarios con capacidad de administrar usuarios suponen un riesgo alto de que se produzcan accesos no autorizados a la aplicación y a los datos.</p>	<p>Modificar la gestión de privilegios dentro de la aplicación de administración de forma que permita limitar las capacidades de administración de usuarios únicamente al personal que esté autorizado para ello.</p> <p>Paralelamente, se debe revisar las acciones realizadas hasta la fecha por todos aquellos usuarios con capacidades de administración, con el fin de verificar que no se han producido acciones no autorizadas y/o erróneas.</p>

**Continuidad del servicio**

El mantenimiento de cualquier sistema requiere la adopción de unas medidas para el caso de que ocurra una interrupción en el funcionamiento del sistema. Se debe comprobar que las entidades cuentan con los procedimientos necesarios para recuperarse de tal interrupción:

- Se debe disponer de una estrategia documentada para la gestión de las copias de seguridad periódicas, tanto de los datos como de los programas de gestión tributaria.
- Deben realizarse pruebas de restauración programadas.
- Hay que definir los plazos de retención y los requisitos de almacenamiento para la información.

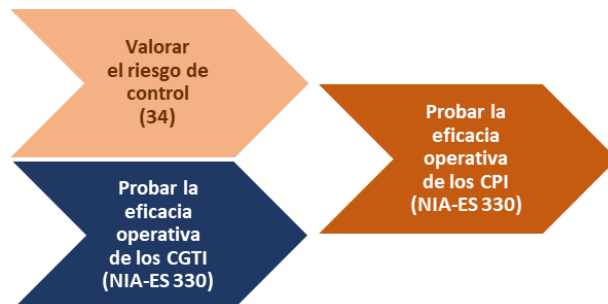
En el caso de que las aplicaciones informáticas de gestión de tributos o parte de los sistemas de información utilizados se hayan contratado en modo Cloud (SAAS, PAAS o IAAS) deberán considerarse las especificidades de los controles de TI en este entorno.

Incluimos a continuación algunos ejemplos:

Deficiencia de control observada	Riesgo	Recomendación
Aunque se dispone de una arquitectura de alta disponibilidad para los servidores de aplicación basada en la existencia de clústeres de servidores, todos los equipos se ubican en un mismo CPD.	En caso de ocurrir un desastre que afectase al CPD, existe el riesgo <b>alto</b> de que se pierdan, de forma irreversible, los sistemas de producción junto con las configuraciones de los sistemas y la lógica de las aplicaciones. La reconstrucción de esta pérdida podría prolongarse durante meses.	Analizar los requisitos relacionados con la continuidad del servicio y la disponibilidad de la información y, en base a estos, desarrollar los correspondientes planes de recuperación ante desastres, que permitan continuar la actividad de la entidad en los tiempos y con los requisitos marcados en caso de ocurrencia de una contingencia grave que afecte a los sistemas principales.
La copia de seguridad de datos y programas se guarda en una caja fuerte ignífuga en el Centro de Proceso de Datos (CPD). En caso de desastre, la copia de datos y programas puede correr la misma suerte que el CPD.	Esta situación implicaría un riesgo <b>alto</b> de pérdida de datos y programas. Además, esto es una obligación legal para los datos de carácter personal de nivel alto.	Contemplar el traslado y almacenamiento fuera del CPD principal de las copias de seguridad que se realicen de datos y programas.
No se ha definido un plan de continuidad de la actividad que permita la recuperación de los procesos de gestión críticos, tras la ocurrencia de una contingencia que afecte a los sistemas de producción, en un tiempo limitado y fijado con anterioridad.	Existe un riesgo <b>alto</b> , en caso de un evento que afecte a los procesos de gestión críticos y los sistemas de información que los soportan, de que no se recuperen las actividades y los datos en los plazos y condiciones requeridas para el logro de los objetivos del Ayuntamiento.	Elaborar y aprobar un plan de recuperación de la actividad, basado en un análisis de riesgos y en la identificación de los activos de TI que son críticos para la entidad, detallando las tareas a realizar para restablecer el servicio, los plazos máximos de respuesta y los periodos de retención de la información.

**11. Revisión de la eficacia operativa de los CPI relevantes**

Una vez verificada la razonabilidad del D+I de los CPI y la eficacia operativa de los CGTI relacionados, que posibilitan el adecuado funcionamiento de aquellos, se debe verificar el adecuado funcionamiento operativo de los CPI relevantes en los que se va a confiar.



Para ello la NIA-ES-SP 1330 (apartado 8) establece que **el auditor diseñará y realizará pruebas de controles con el fin de obtener evidencia de auditoría suficiente y adecuada sobre la eficacia operativa de los controles relevantes si:**

- (a) la valoración de los riesgos de incorrección material en las afirmaciones realizada por el auditor comporta la expectativa de que los controles estén operando eficazmente (es decir, para la determinación de la naturaleza, momento de realización y extensión de los procedimientos sustantivos, el auditor tiene previsto confiar en la eficacia operativa de los controles); o**
- (b) los procedimientos sustantivos por sí mismos no pueden proporcionar evidencia de auditoría suficiente y adecuada en las afirmaciones.**

Además, el apartado 9 de la misma NIA se señala que en el diseño y aplicación de pruebas de controles, **el auditor obtendrá evidencia de auditoría más convincente cuanto más confíe en la eficacia de un control.**

La obtención de evidencia de auditoría sobre la implementación de un **control manual** en un determinado momento **no proporciona evidencia** de auditoría sobre la eficacia operativa del control en otros momentos del periodo que comprende la auditoría.

En el caso de **CPI automatizados**, el auditor comprobará su eficacia operativa tras la identificación y comprobación de CGTI que aseguran el funcionamiento congruente del CPI automatizado (por ejemplo, auditando los controles de acceso y los controles de gestión de cambios) en vez de aplicar pruebas de eficacia operativa directamente sobre los CPI automatizados<sup>6</sup>.

Aunque la realización de pruebas sobre la eficacia operativa de los controles no es lo mismo que la obtención de conocimiento y la evaluación de su diseño e implementación, muchas veces, en entornos de administración electrónica, se utilizan los mismos tipos de procedimientos de auditoría. En consecuencia, **es posible que el auditor decida que resulta eficiente probar la eficacia operativa de los controles al mismo tiempo que se evalúa su diseño y se determina si han sido implementados.** (NIA-ES-SP 1330, A21)

Para más información ver el apartado 11 de la GPF-OCEX 5340.

## 12. Segregación de funciones

Al revisar el proceso de gestión tributaria, un aspecto fundamental es el estudio de la segregación de funciones (SdF), que constituye uno de los principios más importantes del control interno.

Significa que las funciones se distribuyen entre las personas de forma que nadie pueda controlar todas las fases del proceso de una transacción de modo tal que puedan pasar inadvertidas incorrecciones debidas a errores o fraudes. Teóricamente, el flujo de las actividades debería proyectarse de tal forma que el trabajo de una persona sea independiente del de otra o sirva para comprobación de este último.

El objetivo de la segregación de funciones es alcanzado al distribuir las actividades clave del procedimiento de gestión entre varias personas y/o restringir el número de personas con acceso a actividades que sean incompatibles, como por ejemplo la liquidación y la contabilización de ingresos.

En la gestión tributaria serán funciones incompatibles y por tanto no deberían ser desempeñadas por la misma persona las siguientes:

- Liquidación.
- Recaudación.
- Contabilidad.
- Pago.

En la práctica, este principio de SdF ha de conciliarse con consideraciones tales como el volumen, la complejidad y la materialidad de los distintos tipos de operaciones y la secuencia de pasos necesarios para procesarlas. Los aspectos que se deben considerar variarán ampliamente de una entidad a otra. En las entidades de mayor tamaño, las posibilidades de desagregación del trabajo en el proceso de gestión son mayores.

Un aspecto que ha de tenerse siempre en cuenta es el coste de mantenimiento de los controles en relación con el riesgo de las pérdidas por error o fraude que podrían producirse en ausencia de aquéllos. A veces no es posible

---

<sup>6</sup> Apartado A180 de la NIA-ES 315R/GPF-OCEX 1315R.

establecer una adecuada segregación de tareas, sobre todo en entidades de pequeño tamaño, ya que no se dispone de personal suficiente para su implantación, pero en estos casos deben establecerse otro tipo de controles compensatorios<sup>7</sup> que pueden ayudar a mitigar la gravedad de las debilidades de control.

Entre los mecanismos de control disponibles para ayudar a la hora de llevar a cabo controles alternativos a una segregación de funciones eficaz se incluyen:

- Pistas de auditoría/trazabilidad.
- Conciliaciones.
- Informes sobre anomalías.
- Supervisión.
- Auditorías internas de control

En los actuales sistemas altamente automatizados, en los que los usuarios tienen acceso potencialmente a todas las funciones del sistema, el análisis de la segregación de funciones adquiere una importancia especial y debe hacerse una detallada revisión de los riesgos existentes en los permisos de acceso a los sistemas informáticos. Dada su complejidad y “no visibilidad”, en los sistemas informatizados, el análisis de la segregación de funciones muchas veces **solo será posible realizarlo** con la colaboración de personal especializado en auditoría de sistemas de información utilizando herramientas y técnicas automatizadas (HTA).

En el cuadro siguiente se recogen las principales debilidades, en cuanto a segregación de funciones en el proceso de gestión de ingresos tributarios, que pueden entrañar riesgos de errores o irregularidades, y por tanto riesgos de auditoría. Esta tabla es solo un ejemplo de posibles situaciones conflictivas por lo que debe adaptarse a la realidad en cada entidad, analizando como está estructurado el proceso de gestión en cada entidad fiscalizada, ya que las funciones principales y, en consecuencia, sus conflictos, dependen de cada caso específico.

El procedimiento de auditoría lógico consistiría en completar la descripción de los procedimientos de gestión de liquidación y cobro de ingresos tributarios y en cada subproceso hacerse las pertinentes preguntas relacionadas con la gestión de tributos, documentar las respuestas, la evidencia obtenida sobre los posibles conflictos de SdF y sus consecuencias en nuestra evaluación del control interno y valoración del riesgo.

El auditor deberá hacerse las siguientes preguntas y consideraciones:

#	Función	Consideraciones de control / Preguntas de auditoría	Controles posibles/ Recomendaciones	Ejemplos de controles compensatorios
1	Liquidaciones tributarias	Ningún empleado tendrá responsabilidad total para aprobaciones o modificaciones de liquidaciones tributarias incluidas las bajas de derechos.	Un empleado iniciará el proceso o el cambio y otro revisará y autorizará la liquidación o el cambio.	Si la entidad es pequeña o no es posible establecer la segregación de funciones se pueden aprobar procedimientos de revisión periódica de las aprobaciones o modificaciones de liquidaciones tributarias.
2	Liquidaciones tributarias	Los empleados/responsables de la liquidación de los tributos no son los mismos que elaboran las cuentas de recaudación o contabilizan los ingresos.	Un área es responsable de las liquidaciones tributarias y otra contabiliza y/o elabora las cuentas de recaudación.	Informes de control periódicos sobre la gestión de liquidaciones y la contabilización de los ingresos.
3	Maestros de deudores tributarios	Ningún empleado tendrá responsabilidad total para modificaciones en los ficheros maestros de deudores.	Un empleado iniciará el cambio y otro revisará y autorizará el cambio.	Si la entidad es pequeña o no es posible establecer la SdF se pueden aprobar procedimientos de revisión periódica de las altas o modificaciones en los ficheros maestros de deudores.
4	Devolución de ingresos indebidos	Ningún empleado podrá completar y autorizar todas las fases del procedimiento de devolución de ingresos indebidos	Un empleado realizará o autorizará la propuesta y otro autorizará la devolución. El pago será autorizado y controlado por un área o empleado diferente de los anteriores.	Revisión periódica de la devolución de ingresos tributarios. Informes sobre la revisión realizada.

<sup>7</sup> Un **control compensatorio** es aquel que reduce el riesgo de una debilidad, real o potencial, no eliminada por un control directo.

#	Función	Consideraciones de control / Preguntas de auditoría	Controles posibles/ Recomendaciones	Ejemplos de controles compensatorios
5	Cobros de tributos	Los empleados/responsables de control de cobros de deudas tributarias no son los mismos que contabilizan los ingresos tributarios.	Un área o empleado controlará los ingresos en cuentas bancarias y realizará propuestas de contabilización y otra área o empleado contabilizará.	Informes de control periódicos sobre la gestión de cobros y la contabilización de los ingresos.
6	Cobros de tributos	Los responsables de la contabilización de los cobros no son los mismos que los que realizan las conciliaciones bancarias.	Un área o empleado contabilizará y otra área o empleado realizará las conciliaciones.	Informes de control periódicos sobre la gestión de cobros y la contabilización de los ingresos.

Si no es adecuada la segregación de funciones se debe explicar por qué y hasta qué punto puede afectar al riesgo de auditoría. Se deben concretar los riesgos que puede provocar la falta de segregación. Se debe indagar si existen controles compensatorios que mitiguen los riesgos cuando no existe un control directo efectivo.

Si los controles no son eficaces, el auditor deberá realizar procedimientos sustantivos para detectar si se han producido casos de conflicto de SdF. Con HTA podrán realizarse comprobaciones sobre el 100% de las transacciones, de otra forma deberá efectuarse la prueba en base a muestreo.

### 13. Análisis de las interfaces y de los controles sobre ellas (Ver Anexo 1 de la GPF-OCEX 5340)

Normalmente las entidades utilizan sistemas especializados para la gestión tributaria, muchas veces basados en cloud computing gestionado por terceros, distintos de las aplicaciones contables y comparten la información mediante interfaces. Estas interfaces, que sirven para transferir datos de una aplicación a otra, son un área significativa de riesgo para mantener la integridad de los datos económicos.

Por ejemplo, una entidad utiliza una aplicación para gestionar sus tributos y diariamente traspasa toda la información a la aplicación de contabilidad. El programa que se utiliza para hacer la transferencia de datos es la interfaz entre gestión tributaria y contabilidad. Siempre debe comprobarse que los datos se han trasladado a la aplicación contable de forma exacta y completa.

Las interfaces pueden estar automatizadas, ser manuales o mixtas. En todos los casos existe el riesgo de **pérdida o manipulación** de la información, de forma que los datos de la aplicación de origen no coincidan con los que llegan a la aplicación de destino.

Debemos, por tanto:

- Identificar las interfaces existentes que puedan afectar significativamente a las cuentas anuales y suponer un riesgo de auditoría.
- Identificar y evaluar los controles que tenga establecidos la entidad para garantizar la exactitud e integridad de los datos traspasados.
- Diseñar y ejecutar las pruebas de auditoría que se estimen pertinentes para garantizar la exactitud e integridad de los datos.

### 14. Revisión del cumplimiento legal

La auditoría podrá incluir como objetivo, además de la auditoría financiera, la auditoría de cumplimiento de la legalidad.

El objetivo de la auditoría de cumplimiento consiste en verificar que los tributos están liquidados y recaudados de acuerdo con la normativa aplicable. Esta verificación del grado de sometimiento al principio constitucional de reserva de ley afectará no solo al proceso de liquidación tributaria conforme a la normativa reguladora del mismo, sino también al proceso de imposición y ordenación del tributo con relación a la normativa básica de aplicación preceptiva, como puede ser el caso de la aprobación de ordenanzas fiscales por las entidades locales.

Los programas de auditoría recogerán las principales comprobaciones a realizar para asegurar que se ha cumplido, razonablemente, con la normativa.

En estos casos serán aplicables las ISSAI-ES 400 y GPF-OCEX 4000.

#### 15. Importancia relativa

Son aplicables la NIA-ES-SP 1320, la GPF-OCEX 1321, sobre la importancia relativa en las auditorías financieras y la GPF-OCEX 4320 sobre la importancia relativa en las fiscalizaciones de cumplimiento de la legalidad.

Sobre la importancia relativa de las deficiencias de control a efectos de la auditoría ver apartado 14 de la GPF-OCEX 5340.

#### 16. Procedimientos y programas de auditoría

La naturaleza, momento de realización y extensión de los procedimientos de auditoría se determinan de acuerdo con las circunstancias de cada trabajo y deben basarse en el conocimiento de la actividad que realiza el ente auditado, de su organización, de los riesgos valorados, así como en la evaluación del control interno y de la importancia relativa de los saldos en las cuentas anuales.

Los procedimientos de auditoría son las respuestas a los riesgos valorados y por tanto deben ser proporcionales a esos riesgos. Así las áreas de riesgo más alto deben recibir mayor atención y esfuerzo de auditoría.

Los **programas de auditoría** deben ser adaptados a cada entidad, teniendo en cuenta los tributos que se van a auditar y la valoración del riesgo de incorrecciones materiales, e incluirán:

- Pruebas de controles.
- Procedimientos sustantivos (incluyendo procedimientos analíticos y pruebas en detalle).

En las **pruebas de controles** el auditor debe decidir qué controles son relevantes y diseñar y ejecutar pruebas sobre los mismos. Tras realizar estas pruebas, si se han detectado deficiencias de control:

- Se debe evaluar la gravedad de dichas deficiencias
- Modificar la valoración preliminar del riesgo
- Documentar las implicaciones de las deficiencias de control.

Si no se han detectado deficiencias de control, se debe:

- Determinar que la valoración preliminar del riesgo como bajo es adecuada
- Determinar el grado de evidencia que proporcionan los controles sobre la corrección de los saldos.
- Determinar los procedimientos sustantivos a ejecutar.

Los procedimientos de auditoría relacionados con los ingresos tributarios se detallan en un ejemplo en el Anexo 2. Este programa de auditoría ejemplo se debe adaptar a las circunstancias de cada fiscalización.

#### ***Pruebas masivas de datos***

La utilización de aplicaciones informáticas para la gestión de los ingresos y su contabilización permite realizar pruebas masivas de datos para verificar la adecuada gestión, liquidación, recaudación y contabilización. A continuación, se detalla a modo de ejemplo los tipos de pruebas de datos que pueden realizarse a partir de las tablas de las bases de datos de las aplicaciones de gestión tributaria y contabilidad:

- Verificar la integridad de la información facilitada: verificaciones de totales de registros, suma de valores numéricos, numeración de registros, razonabilidad de fechas e importes, ...
- Verificar que existe un adecuado registro de los recibos derivados de liquidaciones de padrones o listas cobratorias: número único identificativo, correlativo. Obtener información sobre el nº de recibos.
- Verificar que la aplicación de gestión de tributos realiza el cálculo de la cuota tributaria correctamente.
- Verificar que, para todas la liquidaciones o autoliquidaciones no ingresadas en el periodo de voluntaria, los subsiguientes cobros se realizan liquidando los porcentajes correspondientes de recargo en función de la situación: 5%, 10% y 20%.
- Verificar que, para todos las liquidaciones o autoliquidaciones no ingresadas en el periodo de voluntaria, se han iniciado los trámites de ejecutiva en plazos razonables.

---

## Guía práctica de fiscalización de los OCEX

### GPF-OCEX 1971 Guía de auditoría del área de ingresos por tributos

---

- Verificar que se registra la información de la gestión recaudatoria en las cuentas de recaudación de forma correcta.
- Analizar los usuarios autorizados para acceder a la aplicación de gestión de tributos. Seleccionar usuarios administradores (todos o una muestra, en función del número) para comprobar que están autorizados. Analizar también quien puede: liquidar, dar de baja liquidaciones, aprobar providencias de apremio, dar de baja providencias apremio, reponer a voluntaria, aprobar bonificaciones, aprobar exenciones, aprobar aplazamientos, aprobar devoluciones de ingresos indebidos, modificar periodos de cobro y modificar tipos impositivos. Verificar segregación de funciones y principio de mínimos privilegios.
- Verificar el correcto funcionamiento de la interfaz entre la aplicación de gestión tributaria y la de contabilidad para la contabilización de las liquidaciones y cobros derivados de la gestión tributaria.

Las pruebas de tratamiento masivo de datos se efectuarán de acuerdo con la GPF-OCEX 5370, Guía para la realización de pruebas de datos.

#### 17. Colaboración de expertos en auditoría de sistemas de información

Para la realización de algunos de los procedimientos de auditoría descritos en esta guía, **los auditores necesitarán, probablemente, conocimientos especializados** proporcionados por auditores de TI para ayudarlos a obtener suficiente evidencia de auditoría adecuada a medida que aumenta la complejidad del entorno de TI. **El OCEX debe garantizar que los miembros del equipo de fiscalización y, en su caso, los expertos externos que formen parte del equipo colectivamente tengan la competencia y las capacidades adecuadas para realizar la fiscalización.**

#### 18. Evaluación de las deficiencias de control interno detectadas

Ver apartado 12 de la GPF-OCEX 5340.

#### 19. Recomendaciones

Ver GPF-OCEX 1735 y apartado 15 de la GPF-OCEX 5340.

#### 20. Documentación del trabajo

Ver NIA-ES-SP 1230, GPF-OCEX 1231 y apartado 16 de la GPF-OCEX 5340.





El auditor debe describir y documentar su comprensión del **proceso de gestión ingresos tributarios** ejecutado por la Entidad. Los objetivos son:

- Comprender los procedimientos (proceso de gestión) establecidos por la entidad para iniciar, autorizar, registrar, procesar e informar (en las cuentas anuales) de las clases de transacciones significativas relacionadas con los ingresos por liquidación de ingresos tributarios.
- Comprender los controles que la entidad auditada ha establecido en el proceso de gestión, analizarlos, y determinar cuáles de ellos pueden considerarse controles relevantes o controles clave (los que contribuyen a reducir el riesgo de auditoría).
- Identificar los procedimientos aprobados por la entidad para gestionar los ingresos tributarios, recaudarlos y contabilizarlos.
- Identificar los órganos y puestos de trabajo que intervienen en la gestión tributaria y sus competencias. Obtener un organigrama detallado.
- Obtener información sobre la aplicación o aplicaciones utilizadas en la gestión de los ingresos y para su contabilización. Identificar interfaces entre aplicaciones.

Para ello puede utilizar este modelo, en el que dicho proceso se descompone en los principales subprocesos o actividades, cada uno de los cuales debe **incluir como mínimo**, la siguiente información, independientemente de que se realice manualmente o de forma automatizada:

- Quién ejecuta el proceso
- Cómo y cuándo se ejecuta
- Qué sistemas informáticos, documentos fuente y registros contables están involucrados
- Cómo se subsanan las transacciones o procesos incorrectos

La descripción realizada en este memorándum debe acompañarse del correspondiente flujograma, ya que ambos se complementan.

Si la entidad dispone de procedimientos formalizados por escrito, la narrativa a realizar por el auditor será tanto más breve cuanto más completos y claros sean aquéllos, que serán archivados y referenciados.

**Nota:** *los subprocesos detallados más adelante son ejemplos y deben modificarse todo lo que sea necesario para adaptarse a las circunstancias de cada entidad fiscalizada.*

#####

**Entidad:** \_\_\_\_\_

**Fecha CCA:** \_\_\_\_\_

**Resumen realizado por (Técnico/fecha):** \_\_\_\_\_

**Revisado por (Auditor/fecha):** \_\_\_\_\_

### **1. Mantenimiento del fichero maestro de deudores-contribuyentes (FMD)**

- a) Los cambios en el FMD se inician de la siguiente forma:
  
- b) Los cambios en el FMD son autorizados de la siguiente forma:
  
- c) Los cambios en el FMD son registrados de la siguiente forma:
  
- d) Los cambios en el FMD son procesados de la siguiente forma:
  
- e) Los cambios en el FMD son reconciliados con la información del proveedor de la siguiente forma:
  
- f) Persona responsable entrevistada

Los procedimientos que hemos realizado para verificar nuestra comprensión (tal como está descrita) del proceso de mantenimiento del FMP han sido los siguientes: *(poner en cada caso lo que corresponda)*

- Hemos revisado los procedimientos de la entidad archivados en el AP.
- Nos hemos entrevistado el \_\_/\_\_/2019 con la persona responsable.
- Hemos realizado una prueba de recorrido archivada en (Ref).
- Hemos realizado un flujograma archivado en (Ref).
- Otros procedimientos.

### **2. Flujograma general (resumido) y detallados**

- Solicitar y/o elaborar. Poner referencia a su archivo.

### **3. Obtención de datos para elaborar y aprobar las liquidaciones de ingresos**

Esta fase del proceso se puede requerir la descripción de diferentes subprocesos en función del objeto de la fiscalización: liquidaciones por padrón y recibo, altas en los padrones, liquidaciones de ingreso directo o autoliquidaciones. Si se refiere a todos los ingresos tributarios se deberán seleccionar aquellos que se consideren más importantes en relación con los objetivos de la auditoría.

Los procedimientos que hemos realizado para verificar nuestra comprensión (tal como está descrita) del proceso de gestión de las compras han sido los siguientes:

### **4. Procedimiento para la tramitación, aprobación y contabilización de bajas de liquidaciones tributarias**

Obtener información detallada y describir el circuito de tramitación, aprobación y contabilización de las bajas de liquidaciones de tributos. Departamentos que participan y responsables de aprobarlas.

Los procedimientos que hemos realizado para verificar nuestra comprensión (tal como está descrita) del proceso de bajas de liquidaciones han sido los siguientes:

**5. Procedimientos de tramitación de aplazamientos y fraccionamientos de deudas tributarias**

Obtener información detallada y describir el circuito de tramitación, aprobación y contabilización de aplazamientos y fraccionamientos de deudas tributarias. Departamentos que participan y responsables de aprobarlos.

Los procedimientos que hemos realizado para verificar nuestra comprensión (tal como está descrita) del proceso de bajas de liquidaciones han sido los siguientes:

**6. Gestión de cobros en voluntaria**

- a) Cuando se ha aprobado un padrón para ponerlo al cobro se inician las siguientes actividades:
- b) Cuando se han aprobado las liquidaciones de ingreso directo se realizan las siguientes actividades:
- c) Cuando finaliza el periodo de voluntaria se realizan las siguientes actividades:
- d) Se dan las siguientes casuísticas habituales que modifican el proceso de gestión en voluntaria: aplazamientos, fraccionamientos, suspensión, ...
- e) Para los cobros en voluntaria se utilizan las siguientes cuentas bancarias que se controlan como se detalla a continuación:
- f) Persona responsable entrevistada

Los procedimientos que hemos realizado para verificar nuestra comprensión (tal como está descrita) del proceso de gestión de cobros en voluntaria han sido los siguientes:

**7. Gestión de cobros en ejecutiva**

- a) El inicio de la gestión de cobro en ejecutiva se realiza de la siguiente manera:
- b) La acción de apremio de valores se realiza de la siguiente forma:
- c) La providencia de apremio se ha dictado correctamente y se han aplicado los recargos y los intereses de demora que corresponden.
- d) El proceso de notificación de la providencia de apremio y resto de actuaciones en ejecutiva se realiza de la siguiente forma:
- e) Para los cobros en ejecutiva se utilizan las siguientes cuentas bancarias que se controlan como se detalla a continuación:
- f) Persona responsable entrevistada

Los procedimientos que hemos realizado para verificar nuestra comprensión (tal como está descrita) del proceso de gestión de cobro en ejecutiva han sido los siguientes:

### **8. Devolución de ingresos**

- a) El proceso de gestión de devolución de ingresos se realiza de la siguiente forma:
- b) La aprobación de devoluciones de ingresos se realiza de la siguiente forma:
- c) El pago de las devoluciones de ingresos se realiza de la siguiente forma:
- d) Persona responsable entrevistada

Los procedimientos que hemos realizado para verificar nuestra comprensión (tal como está descrita) del procesado de devolución de ingresos han sido los siguientes:

### **9. Elaboración, rendición de cuentas de recaudación**

- a) Las cuentas de recaudación las elabora el departamento de ....
- b) las cuentas de recaudación se revisan de la siguiente forma:
- c) Las cuentas de recaudación se aprueban de la siguiente forma:

### **10. Contabilización de los ingresos en voluntaria, ejecutiva y devoluciones de ingresos indebidos**

- a) La aplicación utilizada para la contabilización de ingresos es la siguiente:
- b) El proceso de contabilización de los ingresos en voluntaria y en ejecutiva es el siguiente:
- c) La interfaz entre la aplicación de gestión de ingresos funciona de la siguiente forma, en su caso:
- d) Los controles que se realizan sobre la contabilización de ingresos son los siguientes:
- e) Las conciliaciones bancarias se realizan de la siguiente forma
- f) Persona responsable entrevistada

Los procedimientos que hemos realizado para verificar nuestra comprensión (tal como está descrita) del proceso de contabilización han sido los siguientes:

### **11. Soporte informático**

Obtener información de las características básicas de las aplicaciones: indicar si son comerciales o de desarrollo propio, responsables funcionales de la aplicación, responsables en TI. Identificar los puntos del procedimiento en el que se producen traspasos (manuales o automáticos) entre una aplicación y otra (interfaces) que no se hayan comentado en apartados anteriores. Relacionar todas las interfaces.

La entidad utiliza las siguientes aplicaciones para la gestión del proceso:

Gestión de ingresos:

Gestión de tesorería:

Contabilidad:

Los procedimientos que hemos realizado para verificar nuestra comprensión (tal como está descrita) del proceso de contabilización han sido los siguientes:

### **12. Observaciones significativas, riesgos significativos, hallazgos y conclusiones**

Los procedimientos que hemos realizado para adquirir nuestro conocimiento del proceso han sido los siguientes:  
*(poner en cada caso lo que corresponda)*

- *Hemos revisado los procedimientos de la entidad archivados en el AP.*
- *Nos hemos entrevistado el \_\_/\_\_/202\_ con la persona responsable \_\_\_\_\_.*
- *Hemos realizado una prueba paso a paso en (Ref).*
- *Hemos realizado un flujograma archivado en (Ref).*
- *Otros procedimientos: \_\_\_\_\_*
- *Deficiencias de control detectadas: \_\_\_\_\_*
- *Recomendaciones realizadas: \_\_\_\_\_*



(Al diseñar los programas de trabajo, se seleccionarán aquellas pruebas que respondan mejor a los riesgos detectados en la planificación de la auditoría y se adaptarán a las circunstancias de la entidad. El ejemplo siguiente es un programa ejemplo meramente orientativo, para la auditoría de un ayuntamiento, que debe adaptarse a las circunstancias de cada auditoría.

Cada OCEX podrá sustituirlo por los que tenga establecidos como estándar.)

### Hoja sumaria

1. Confeccionar las hojas sumarias para cada uno de los capítulos de ingresos tributarios (capítulos 1,2 y3), a nivel de artículo y concepto con detalle de su ejecución presupuestaria. Calcular el grado de ejecución y de realización.
2. Analizar comparativamente la ejecución de los capítulos del ejercicio actual, con la del ejercicio anterior.  
Efectuar una revisión analítica de las cuentas de ingresos, al nivel de desglose que se considere necesario o adecuado e investigar las variaciones significativas de saldos interanuales (según los casos podrá hacerse el análisis de los tres últimos ejercicios), obteniendo y documentando las razones de dichas variaciones y su coherencia.  
Comentar la ejecución: significatividad, modificaciones de las previsiones iniciales, grado de ejecución y de cumplimiento (cobro), ...
3. Comprobar las cifras de la liquidación con el balance y la cuenta de resultados. Respecto a los ingresos, comprobar el cuadro de conciliación del resultado económico-patrimonial con el resultado presupuestario que consta en la Memoria. Explicar las diferencias.

### Memoria

4. Extraer de la memoria, y añadir aquí (pdf) o referenciar, la información referente a este apartado de la liquidación.  
Analizarla y comprobar que contiene toda la información aplicable requerida por el PGCP e Instrucción de Contabilidad

### Normativa de ingresos

5. Detallar en un p/t la normativa más importante reguladora de los ingresos aplicable al ejercicio. A tal efecto puede utilizarse el p/t del año anterior debidamente actualizado.  
Comentar o resumir en un Word los aspectos más significativos de dichas normas, especialmente las nuevas, y sus incidencias en el ámbito de la fiscalización.

### Conocer y comprender los procedimientos de gestión de ingresos tributarios y recaudación

6. Conocer y comprender los procedimientos de gestión de ingresos tributarios y recaudación:
  - a. Solicitar, si existen, procedimientos de gestión tributaria y de recaudación.
  - b. Revisar el procedimiento de gestión tributaria con una prueba paso a paso y describirlo en una narrativa (ver anexo 1 de la GPF-OCEX 1971).
  - c. Realizar un flujograma de los procesos de gestión de ingresos más relevantes.
  - d. Describir las aplicaciones informáticas y el soporte informático en general de la gestión tributaria.
  - e. Complimentar la revisión del control interno y resumir los puntos débiles de control interno detectados.
  - f. Analizar conflictos de segregación de funciones en los procesos más relevantes
  - g. Hacer un resumen de los aspectos susceptibles de mejora y proponer las sugerencias y recomendaciones que se consideren oportunas para mejorar el control interno y comentarlas con la dirección.
  - h. Documentar el trabajo según el Anexo 1 de esta guía GPF-OCEX 1971.

Respecto de la recaudación señalar:

- i. La legalidad de las tareas contratadas o delegadas, si es el caso.
  - j. Fianzas prestadas.
  - k. Periodicidad de los ingresos.
  - l. Rendición de cuentas y prescripción.
  - m. Archivar la documentación justificativa.
7. Si hay informes de auditoría de años anteriores, revisarlos y hacer el seguimiento de las deficiencias y de las recomendaciones. Concluir sobre el estado actual e impacto en la presente fiscalización.
  8. Realizar un resumen de los principales riesgos inherentes identificados en el proceso de gestión, valorar los riesgos inherentes y elaborar el espectro de riesgo inherente (si no se ha elaborado al planificar la auditoría de las cuentas anuales). Determinar qué riesgos son significativos.
  9. Revisar la valoración del riesgo para esta área.
  10. Identificar los CPI relevantes relacionados con el proceso de gestión de ingresos y los CGTI que los soportan.
  11. Se debe realizar o discutir este análisis en una reunión del equipo (ver GPF-OCEX 1513).

#### Revisar los CGTI

**NOTA:** *Este paso de programa se cumplimentará por el auditor de sistemas cuando esté prevista su colaboración.*

*En las fiscalizaciones recurrentes más importantes, cuando esté previsto en el plan anual o en función de las circunstancias se considere necesario ampliar el alcance de la revisión del proceso y aplicación de gestión de ingresos se deberá recabar la colaboración del auditor de sistemas.*

*En los ayuntamientos pequeños probablemente no sea fácil cumplimentar este paso.*

12. Solicitar la colaboración de expertos en auditoría de sistemas.
13. Ver el trabajo hecho por el equipo de fiscalización en el paso de programa: **Conocer y comprender los procedimientos de gestión**, y comentarlo entre el auditor y el auditor de sistemas. Completar la revisión del proceso/aplicación de gestión realizada por el equipo de fiscalización.
14. Realizar las pruebas de eficacia del diseño y de eficacia operativa (pruebas de controles).
15. Concluir sobre la situación de los CGTI, su impacto en los CPI y si tiene efecto en la opinión de auditoría.

#### Pruebas de controles de CPI

16. Revisar los CPI y realizar pruebas de controles.

#### Procedimientos sustantivos

17. Obtener copia de la totalidad de las ordenanzas fiscales en vigor y acuerdos de exacción.
18. Para una muestra de las ordenanzas en vigor seleccionadas de acuerdo con el Auditor, comprobar la adecuación de las mismas a lo determinado al respecto en el TRLRHL.
19. Archivar copia de la documentación sobre cuentas de recaudación del ejercicio, informes del tesorero, interventor, comisión liquidadora y acuerdos de aprobación. Verificar que los informes y acuerdos coinciden con los datos que se desprenden de las cuentas.

A la par que se comprueban aritméticamente las cuentas de recaudación, obtener los principales indicadores que permitan una revisión analítica de las cuentas.

20. Obtener en el Ayuntamiento la documentación justificativa de la Cuenta de Recaudación:
  - a) Cuentas de recaudación del ejercicio anterior que justificarán las columnas de saldos y pendientes de ejercicios anteriores.



- b) Relación de cargos del ejercicio que justificarán los cargos en voluntaria y en ejecutiva.
  - c) Cartas de pago del ejercicio acreditativas de los ingresos en voluntaria y en ejecutiva.
  - d) Relaciones de datas por bajas, por insolvencias, por adjudicaciones y por otros motivos.
  - e) Relaciones de valores pendientes de cobro que obren en poder de los recaudadores.
21. Comprobar las cuentas de recaudación con la documentación justificativa del punto anterior.
22. Seleccionar unas liquidaciones correspondientes a dichos ingresos y comprobar que se ha cumplido lo estipulado en la ordenanza respecto a su cuantificación.
23. Para los ingresos que se liquidan a través de padrón:
- a) Comprobar que los padrones se aprueban y publican a efecto de notificación.
  - b) Archivar las fotocopias de las últimas hojas de cada uno de los padrones del ejercicio.
  - c) Comprobar su cuadro con las respectivas cuentas contables.
  - d) Para dichas cuentas, a partir del libro mayor de concepto presupuestario de ingresos, analizar los principales derechos reconocidos en el ejercicio que no se correspondan con el cargo del padrón, y comprobar su adecuada liquidación e imputación contable.
  - e) Comprobar si finalizado el período de cobro en voluntaria, el Recaudador confecciona la relación nominativa de deudores por los recibos pendientes e intervención certifica la deuda de los ingresos pendientes, para su posterior diligencia en vía de apremio. Analizar las fechas de las certificaciones en relación con la fecha de finalización del período voluntario.
  - f) Comprobar si el Tesorero en base a las certificaciones anteriores expide la providencia de apremio. Analizar las fechas del apremio en relación con la fecha de finalización del período voluntario y con la fecha de las certificaciones.
  - g) Comprobar si las certificaciones apremiadas por el Tesorero han sido cargadas al recaudador. Analizar la fecha del recibí.
  - h) Verificar la aplicación de los recargos e intereses exigibles para los ingresos realizados con posterioridad a la fecha de vencimiento del período voluntario.
  - i) Comprobar que la providencia de apremio se notifica con todos los requisitos exigidos en la Ley General Tributaria.
24. Obtener una copia del libro mayor del presupuesto de ingresos de aquellos conceptos no recogidos en el apartado anterior. Seleccionar liquidaciones de contraído previo y contraído simultáneo. Para los conceptos correspondientes a las liquidaciones seleccionadas comprobar la coherencia entre mayor y liquidación.
25. A partir de la muestra anterior y a partir de sus documentos contables, comprobar:
- a) Formalización adecuada. (Documento contable y firmas).
  - b) Justificantes de ingreso y cobro, en su caso.
  - c) Aplazamientos y fraccionamientos con su siguiente repercusión contable.
  - d) Las liquidaciones practicadas se ajustan a la ordenanza.
26. Para una muestra de expedientes tributarios de ingreso directo liquidados en el ejercicio y no satisfechos en periodo de cobros en voluntaria, comprobar el cumplimiento de los trámites de los puntos e), f), g), h) e i) del apartado 22.

**Revisión muestra DR y MI de ingresos tributarios**

27. Seleccionar una muestra significativa de documentos de reconocimiento de derechos “DR” y de cobros “MI” a partir del libro mayor en soporte informático remitido por la IG.
28. Solicitar los ficheros de las bases de datos de ingresos objeto de fiscalización. Planificar y ejecutar pruebas de masivas de datos para verificar la integridad de los derechos reconocidos y cobros efectuados.  
  
Explicar los criterios y procedimiento de extracción y selección. Al seleccionar la muestra se tendrán en cuenta las transacciones ya revisadas con motivo de otras pruebas en otras áreas.
29. Solicitar la documentación de la muestra seleccionada para revisar.  
  
Añadir un p/t describiendo los aspectos revisados de la muestra, que como mínimo incluirán: a) correcto reconocimiento e imputación contable; b) correcto soporte documental; c) cobro posterior, en su caso.
30. Analizar el cumplimiento de la orden anual reguladora de las operaciones de cierre del ejercicio, y su efecto en la correcta contabilización de los ingresos.

**Revisión derechos pendientes de cobro**

31. Coordinadamente con el resto de apartados de esta área, analizar los derechos pendientes de cobro y seleccionar una muestra de ellos para detectar deficiencias en su reconocimiento, así como posibles problemas de cobrabilidad. Analizar el soporte documental y cuadrar los importes correspondientes con las cuentas de recaudación. Determinar los que en principio deberían ser objeto de consideración como de dudoso cobro.
32. Anulaciones posteriores. Solicitar por escrito que nos informen de las anulaciones producidas hasta la fecha de derechos reconocidos en el ejercicio y anteriores. Analizar, revisar y comentar la información al respecto.
33. De los expedientes de bajas de derechos de presupuesto corriente, verificar si están perfectamente soportadas documentalmente, con especial atención a aquellos que deriven en devolución del cobro.
34. De la relación de datas por insolvencias y otras causas, seleccionar una muestra y comprobar los expedientes de declaración de fallidos o, en el caso de no existir responsables solidarios ni subsidiarios, de crédito incobrable. Analizar las actuaciones y documentación justificativa. Comprobar su contabilización.
35. Analizar una muestra de expedientes de prescripción de deuda. Pronunciarse sobre las causas.
36. Requerir al Ayuntamiento que justifique que los valores pendientes de cobro con antigüedad superior a 4 años no se encuentren prescritos.

**Seguimiento informes anteriores**

37. Realizar un seguimiento de las recomendaciones del informe de fiscalización anterior y comentar la situación actual.

**Conclusión área ingresos tributarios**

38. Redactar las conclusiones del área:
  - a) Organización de la gestión tributaria y recaudación
  - b) Contabilización y ejecución de los ingresos tributarios.
  - c) Confeccionar un cuadro resumen donde se recojan los ajustes y reclasificaciones detectados durante el trabajo realizado en esta área.
  - d) Comentar con los órganos gestores y con la IG los aspectos más importantes de nuestras conclusiones anotando sus comentarios.

La conclusión global de auditoría del área debe ser inequívoca y debe expresar la opinión profesional (basada en la evidencia suficiente y adecuada obtenida tras todas las pruebas de auditoría realizadas) sobre si la cifra de ingresos tributarios y otras revelaciones relacionadas que reflejan las cuentas anuales es completa, exacta, está adecuadamente contabilizada y si la gestión ha sido conforme con la normativa.