Guía práctica de fiscalización de los OCEX

GPF-OCEX 1957 Guía de auditoría del área de Tesorería

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

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 la Tesorería. La gestión de la tesorería es el resultado final de la gestión de gran cantidad de transacciones del resto de áreas de ingresos y gastos, de las actividades de inversión y de financiación, con las que está enlazada mediante múltiples interfaces automatizadas. La gestión de cobros y pagos con las entidades financieras también está automatizada y cuenta con interfaces informatizadas entre la aplicación de tesorería propia con las entidades financieras.

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 de la tesorería 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 la información (CGTI) que los respaldan.

Esta guía es aplicable en las auditorías del área de tesorería y su **objetivo** es ayudar al auditor a:

- Adquirir un conocimiento profundo de los procedimientos/procesos de gestión establecidos por la entidad para la gestión de los cobros, pagos y el control de las cuentas de tesorería.
- 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 sustantivos mínimos recomendados para la fiscalización del área de tesorería, incluyendo un contenido orientativo del programa de auditoría.
- Documentar los procedimientos ejecutados, la evidencia obtenida y las conclusiones alcanzadas.

La adecuada comprensión de esta guía **requiere el conocimiento previo de las NIA-ES-SP 1330, 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 cualquier entidad del sector público.

En las entidades de menor tamaño y complejidad 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 guía es aplicable a la fiscalización/auditoría del área de Tesorería. En particular las cuentas a las que son de aplicación las orientaciones de la presente guía son:

Entidades que aplican el PCG y sus adaptaciones	
570, 571	Caja
572-575	Bancos e instituciones de crédito
576	Inversiones a CP de gran liquidez

Entidades que aplican el PCGP y sus adaptaciones	
570, 574	Cajas
571, 573, 575, 577	Entidades bancarias
578, 579	Otras cuentas de tesorería
558	Pagos a justificar
554	Cobros pendientes de aplicación
555	Pagos pendientes de aplicación
550	Pagos en formalización
558	Anticipos de caja fija

Hay que tener presente que las cuentas de tesorería están íntimamente relacionadas con la mayor parte de las operaciones de ingresos, gastos, financiación, etc. de cualquier entidad, por lo que será necesario conocer dichas interrelaciones.

4. Objetivos de la auditoría del área

El **objetivo general de auditoría** del área consiste en determinar si los saldos de las cuentas de tesorería han sido adecuadamente gestionados y presentados en las cuentas anuales fiscalizadas, si estas reflejan de forma completa y exacta dichos saldos, 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 saldos de tesorería 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.

Las **afirmaciones** y los **objetivos detallados** de auditoría relacionados con la tesorería son:

Afirmación		Descripción/Objetivo
Existencia	E	Los saldos de tesorería (caja y bancos) existen realmente. Los cobros y pagos del periodo son reales.
Derechos y obligaciones	DO	Los saldos de tesorería (caja y bancos) son propiedad/titularidad de la entidad y no hay restricciones que limiten su disponibilidad.
Completitud	C	Los saldos de tesorería incluyen los fondos en todas las delegaciones/localidades, y todo tipo de fondos, en custodia, en tránsito, cajas fijas, etc. No se han producido omisiones. La totalidad de los cobros y pagos se han contabilizado.
Exactitud, valoración e imputación	Ex	Los saldos de tesorería están adecuadamente valorados. Los cobros y pagos son registrados prontamente en importe, periodo y cuentas correctas.
Clasificación	Cl	Los saldos de tesorería están adecuadamente clasificados en las cuentas anuales.
Presentación	P	La memoria recoge toda la información requerida sobre los saldos de tesorería.
Legalidad	L	Se han observado todas las normas legales aplicables a las transacciones de efectivo.

Por la propia naturaleza de las cuentas de tesorería, su valoración no debe constituir ningún problema, ya que normalmente están auto valoradas, por ser moneda de curso legal.

El programa detallado de auditoría debe atender a estos objetivos y adaptarse a las características de la entidad y a los riesgos de auditoría.

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, debe expresar la opinión profesional (basada en la evidencia obtenida tras todas las pruebas de auditoría realizadas) sobre si la cifra de tesorería 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 de tesorería y de la aplicación TI que lo soporta

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

Así, 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 la tesorería 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 gestión de tesorería de la entidad, incluidos sus datos e información, los recursos que se deben utilizar en esas actividades y obtener conocimiento sobre:

(a) el modo en que la información fluye por el sistema de información, 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 tesorería 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 la tesorería, tanto cobros como pagos.

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, o bien 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 la tesorería

Se recomienda vivamente 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).

La gestión de la tesorería se encuentra condicionada por todo el proceso de gestión presupuestaria-contable, pues muchos de los controles que afectan a la tesorería se ubican en las fases previas de este proceso (por ejemplo, para que se pueda pagar un gasto debe haber sido previamente presupuestado, autorizado, dispuesto, justificado, fiscalizado y contabilizado).

En una entidad de tamaño mediano o grande, el proceso de gestión de tesorería 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 de tesorería con el resto de las aplicaciones de gestión, en especial con la contable.

Para identificar y analizar las aplicaciones de gestión y las interfaces existentes será conveniente contar con la colaboración de expertos en auditoría de sistemas de información.

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 deberá identificar y valorar los RIM en los estados financieros y/o el área de tesorería 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 tesorería en particular, pero que pueden afectar a muchas afirmaciones (por ejemplo, (a) si la entidad tiene un departamento de tesorería claramente infradotado 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 de la tesorería 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 tesorería 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. (En el área de tesorería por la naturaleza líquida del activo a proteger **el riesgo de fraude mediante el uso de las TI es especialmente relevante**).

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 analizados, a la pregunta:

¿**Qué puede ir mal** en el proceso de gestión de tesorería 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.

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

#	Riesgos inherentes	Función	Afirma-ción	Probabilidad (1 a 10)	Magnitud (1 a 10)	Valoración del R.I.(PxM)
RT01	Apropiación indebida de los fondos de bancos, por ejemplo, realizando transferencias fraudulentas a cuentas ajenas.	**Gestión de tesorería**	E, L			
RT02	Existen cuentas bancarias no contabilizadas ni controladas.		C, L			
RT03	Existen cuentas bancarias sin movimiento en los últimos años.					

#	Riesgos inherentes	Función	Afirma-ción	Probabilidad (1 a 10)	Magnitud (1 a 10)	Valoración del R.I.(PxM)
RT04	Se producen cambios de cuentas con excesiva frecuencia					
RT05	Existen personas autorizadas para disponer en cuentas sin tener competencia para ello (porque nunca la tuvieron o porque han dejado de tenerla).		E, L			
RT06	Existen firmas solidarias para disponer en cuentas, lo que representa un riesgo de disposición indebida de fondos.		E			
RT07	Los datos del FMT no son exactos.	**Mantenimiento del FMT (Fichero Maestro de Terceros)**	E			
RT08	Se producen altas y modificaciones no autorizadas en el FMT que pueden derivar en pagos a terceros incorrectos o fraudulentos.		E, L			
RT09	Pagos realizados por bienes o servicios no recibidos, pagos inexactos o excesivos.	**Pagos**	Ex, L			
RT10	Pagos realizados por personas no autorizadas o sin competencia (que acceden a la aplicación de pagos). Incluye los fraudes por suplantación de identidades en el sistema o en los correos electrónicos para el envío de órdenes de pago. Falsificación de órdenes de pago.		E, L			
RT11	Realizar pagos excesivos o indebidos en cuentas extrapresupuestarias.	**Pagos extrapresu-puestarios**	E, L			
RT12	Modificación no autorizada de la información en la interfaz manual ERP[1]-Bancos para realizar pagos, ya que la carpeta donde se deposita transitoriamente el fichero Cuaderno 34-XML puede no estar debidamente protegida frente a accesos no autorizados.	**Interfaz de pagos**	L			
RT13	Pagos indebidos por modificación no autorizada de la información en la interfaz automatizada ERP-EDITRAN-Bancos para realizar pagos.		L			
RT14	Omitir o retrasar el registro de las entradas de efectivo/cobros.	**Cobros**	Ex			
RT15	Detraer las entradas de efectivo, una vez registradas.		E, L			
RT16	Ocultar operaciones introduciendo abonos no justificados (p. e., bonificaciones o exenciones) o anulaciones simuladas para ocultar la apropiación indebida de los cobros. Que se cancelen cuentas a cobrar como si fueran incobrables, sustrayendo los fondos o facturando por importes inferiores a los normales para disimular las cantidades sustraídas.		E, L			

[1] ERP: Enterprice Resource Planing. Es el software utilizado por la organización para gestionar sus actividades empresariales diarias como pueden ser, entre otras, la tesorería

#	Riesgos inherentes	Función	Afirma-ción	Probabilidad (1 a 10)	Magnitud (1 a 10)	Valoración del R.I.(PxM)
RT17	Contabilización errónea o fraudulenta de saldos pendientes de cobro o pago y de movimientos bancarios	**Contabilidad**	Ex			
RT18	Ocultar operaciones no autorizadas o fraudulentas mediante la falsificación de conciliaciones bancarias.		Ex, L			
RT19	La interfaz de la aplicación de tesorería con la aplicación contable (en los casos que no sea la misma aplicación) no garantiza la integridad de los datos, lo que puede posibilitar la comisión de fraudes.		E Ex L			
RT20	No se registran todos las entradas y salidas de efectivo en las cajas. Se pueden detraer efectivo de forma no autorizada sin que sea detectado	**Caja**	E, Ex, L			
RT21	Apropiación indebida de los fondos de caja. Los saldos de efectivo no están protegidos		E, L			

Aunque no son objeto de estudio en esta guía no debe pasarse por alto también los riesgos relacionados con los avales contraídos y las fianzas (con relación a su custodia, conciliación entre contabilidad y documentación de los constituidos y cancelados, sobre si se cumple la normativa, riesgos en gestión de avales en formato digital, etc).

6.3 Determinar los riesgos significativos en el espectro de riego 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 de tesorería 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 *(en un gran ayuntamiento, con cientos de miles de movimientos de tesorería, revisar las conciliaciones bancarias manualmente probablemente 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 tesorería

El área de tesorería ha sido siempre un área propensa a que se cometan fraudes e irregularidades de distinto tipo. La razón es muy sencilla, es más fácil robar dinero en efectivo o en bancos que un inmueble, por ejemplo.

Las amenazas tradicionalmente eran internas, pero con la utilización intensiva de los sistemas de información y la interconexión por internet, además de incrementarse aquellas, han aumentado de forma exponencial las amenazas externas debido a las vulnerabilidades que puede ofrecer un sistema de información mal protegido.

Tanto las amenazas internas como las externas pueden ser minimizadas con un adecuado sistema de control interno implantado de forma efectiva.

Pero, 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 es tan solo un cascarón vacío**.

Riesgo de fraude manipulando el fichero maestro de terceros (FMT)

Uno de los mecanismos más utilizados para cometer un fraude ha consistido, tradicionalmente, en la manipulación indebida de los datos relativos a los terceros a los que hay que pagar determinadas cantidades por cualquier motivo, a priori legítimo, bien sea como pago por la compra de bienes o servicios, por nóminas, subvenciones, etc. Dichos datos, incluyendo los relativos a las cuentas bancarias donde se realizan los pagos, se mantienen en un fichero que denominamos Fichero Maestro de Terceros, el cual siempre ha sido objeto de protección especial por parte de los sistemas de control interno.

Este riesgo de fraude clásico tenía como principales amenazas los usuarios internos. La utilización de sistemas de información interconectados y en particular el uso de internet ha ocasionado un aumento de las **amenazas internas y** sobre todo las **externas** que pueden provenir de cualquier parte del mundo, y por tanto la multiplicación de los riesgos de fraude y la exigencia de una sólida red de controles para proteger la seguridad y la integridad del FMT.

Como señala Godino y Menéndez[2], una de las funciones clave de la Tesorería, como es la tramitación de pagos, está en el punto de mira de la delincuencia organizada, la cual, aprovechándose de las vulnerabilidades de las Administraciones públicas, opera de forma fraudulenta para suplantar identidades y de este modo desviar los pagos dirigidos a los verdaderos acreedores, produciendo con ello un menoscabo en las arcas públicas al tratarse de un pago que no tiene carácter liberatorio.

Ver más información en el Anexo 1A.

Ciberriesgos

Los fraudes derivados de malas praxis relacionadas con la seguridad de los sistemas de información son de muy distinto tipo:

- Fraude del CEO (se vulneran los procedimientos y se hacen pagos a IBAN distintos a los del FMT). Este fraude utiliza métodos de ingeniería social para vulnerar los procedimientos y los controles, con la finalidad de inducir pagos a proveedores y/o cuentas que no están en el FMT[3].
- *Phishing*. Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas. Con este método se consigue hacer cambiar el IBAN existente en el FMT de un proveedor, para pagar una deuda real a la cuenta de los defraudadores. Para culminar el fraude hay que vulnerar los procedimientos y controles[4].

[2] **Seguridad y eficacia en los pagos. El fraude bancario. Cómo minimizar los riesgos y evitar responsabilidades derivadas**. Rosario Godino López y Marina Menéndez Miralbés, Revista de Estudios Locales nº 271. Este artículo analiza en profundidad toda la problemática relacionada con los FMT y por eso es recomendable su lectura.

[3] El caso más mediático fue el perpetrado hace unos pocos años a una empresa municipal de transporte urbano en el que defraudaron 4,5 millones de euros que no se han recuperado.

[4] La implantación del protocolo DMARC en los correos electrónicos mitiga este riesgo. Ver nota al pie nº 10.

- Ataques *Man in the middle*. Consiste en interceptar la comunicación entre un emisor y un receptor, pudiendo espiar o modificar la información con fines maliciosos.
- Acceso no autorizado a información. Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
- Suplantación de identidad (por métodos distintos al *phishing*). Se accede al sistema y se suplanta la identidad de un usuario autorizado para hacer cambios indebidos en el FMT o para hace pagos no autorizados.[5]
- Modificación no autorizada de información. Ej: modificación del IBAN por un atacante empleando credenciales sustraídas de un sistema.
- Los CGTI son muy débiles o inexistentes y se puede acceder sin dificultad al FMT u otros procesos y/o registros para hacer cambios indebidos. (Ver apartado 10).

6.6 Otros riesgos

Una fuente de información interesante, que periódicamente proporciona información sobre fraudes cometidos, son las noticias de prensa. Tomando una noticia del 7 de diciembre de 2023 sobre un informe emitido por la Intervención General de una comunidad autónoma se puede hacer un breve catálogo básico de riesgos de fraude (omitimos las entidades fiscalizadas, pero según esa noticia afectan en distinto grado al 90% de las entidades auditadas y un 46% tienen un nivel de riesgo alto en el área de pagos), según aquella:

- Las empresas de la Comunidad sin control en los pagos a proveedores (titular).
- La Intervención alerta del riesgo de fraude o error en los pagos (subtítulo)
- La Intervención detecta 22 entidades con un nivel de riesgo alto en el área referida a los pagos.
- Las principales incidencias se refieren a la ausencia de procedimientos formalmente aprobados de **verificación de los datos de terceros** y sus cuentas bancarias, así como la **ausencia de identificación electrónica segura del tercero y de la cuenta bancaria destinataria del pago**.
- Deficiencias en la emisión y firma de las órdenes de pago.
- Se recomienda el establecimiento de medidas técnicas que posibiliten que **las conciliaciones de saldos bancarios y contable se realicen de manera informática y con periodicidad no superior a la semana**.
- Se recomienda implantar sistemas de evaluación de riesgos que permitan identificar y medir aquellos que afectan al área de gestión financiera y adaptar el sistema de control interno de forma que se evite o reduzca la probabilidad de su ocurrencia e impacto.

7. Identificación de los controles de procesamiento de la información 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.

[5] José Manuel Farfán Pérez en el artículo **Gestión de pagos en la Administración Local: ciberseguridad y validación de cuentas**, en "El Blog de espublico",señala que la directiva PSD2 ha aumentado la seguridad en las transacciones, pero a la vez se está produciendo un fenómeno de **incremento de la ciberdelincuencia en los procesos anteriores al pago, a través de la suplantación de identidad en los procesos de acreditación de terceros**. Las malas prácticas han posibilitado una creciente proliferación de fraudes de suplantación de identidad y los pagos a un tercero no acreedor.

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[6].** 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 de tesorería, 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.

- **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.

  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 se 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 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.

[6] Apartado A148 de la NIA-ES 315R/GPF-OCEX 1315R.

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 saldo contable	Existencia		
	Derechos y obligaciones		
	Completitud		
	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 tesorería

La entidad auditada debe mantener un adecuado control interno sobre el dinero en efectivo dado que la mayoría de las transacciones finalizan en movimientos de caja y bancos, y la falta de controles puede incentivar actividades fraudulentas.

En la **organización interna** de una entidad se deben contemplar requisitos como los siguientes:

- El departamento de tesorería debe estar separado de cualquier otro.
- El tesorero no debe realizar funciones de cuentas a cobrar y a pagar.
- Los empleados del departamento de tesorería deben tener claramente definidas sus funciones y responsabilidades.
- Debe existir una política financiera adecuada, por escrito, en cuanto a las cuentas bancarias, autorizaciones, etc.

Los **principales controles** en el área de tesorería incluirán (relación no exhaustiva):

- Los **procedimientos** de gestión de la tesorería (cobros, pagos o transferencias, mantenimiento del fichero maestro de terceros, etc) han de constar por escrito y reflejar los límites y autorizaciones.
- Existencia de una adecuada **segregación de funciones** en todo el proceso.
- Las firmas autorizadas para disponer en bancos han de ser siempre **mancomunadas**.
- Las operaciones de disposición de fondos a través de las plataformas de las entidades financieras se regularán en los pliegos de contratación de las cuentas bancarias de forma que se requerirá la remisión de un documento electrónico firmado electrónicamente por las personas autorizadas para que la entidad financiera pueda ejecutar las órdenes de pago mediante la operativa de la banca electrónica.

  Las condiciones de los pliegos o, en su defecto, las instrucciones cursadas por escrito a las entidades financieras deben detallar las verificaciones que son responsabilidad de la entidad financiera (verificar la autenticidad de firmas de las órdenes de pago, verificar la autenticidad e integridad de los ficheros de pago, …).
- **Controles de acceso**:
  - Solo los funcionarios de Tesorería deben tener acceso a la aplicación de gestión de tesorería o a las funcionalidades para el área de tesorería de la aplicación de contabilidad 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 o funcionalidades de tesorería se revisan periódicamente para garantizar que los privilegios estén restringidos al personal adecuado.
  - Sólo los funcionarios de intervención tienen acceso a las funciones de fiscalización de ingresos y pagos.
  - Sólo los funcionarios de tesorería que lo necesiten para ejercer sus funciones deben tener acceso a la banca electrónica de las cuentas de la entidad.
  - Las autorizaciones de acceso y modificación del fichero maestro de terceros contemplan la segregación de funciones respecto a la gestión de ingresos y pagos (en una entidad local, por ejemplo, intervención realiza el alta y modificación de los ficheros de terceros y cuentas bancarias y los funcionarios de tesorería no tienen acceso a esos menús de la aplicación).
- Controles sobre los **cobros**:
  - De haber cobros en metálico (no recomendable, con carácter general), los cobros deben ingresarse en el banco inmediatamente, en cuentas distintas a las que se emplean para realizar pagos. Debe aplicarse el principio de proporcionalidad y si los cobros por caja son residuales no será preciso realizar los ingresos diariamente. Desde el punto de vista del auditor tendremos en cuenta los criterios de importancia relativa definidos en la planificación y el juicio profesional, para determinar la frecuencia recomendable en cada caso.
  - Se han de usar recibos numerados correlativamente para la recepción de ingresos, y establecer un adecuado control de los recibos en blanco.
  - Todas las operaciones se registran pronta y exactamente en la contabilidad o en registros auxiliares y se emiten los informes apropiados.
- Realizar **conciliaciones bancarias** periódicamente.

  Las conciliaciones bancarias constituyen un aspecto esencial en el control interno de la tesorería. Consisten en poner de manifiesto las diferencias entre los registros contables de la entidad y los saldos del banco, según los extractos, a una fecha determinada.

  Tradicionalmente se hacían en los formularios establecidos al efecto por una persona diferente de la que realiza los registros contables y el manejo de fondos. En un entorno informatizado deben realizarse automáticamente, como mínimo semanalmente, y preferiblemente de forma diaria (en las entidades grandes desde luego).

  Deben ser revisadas y firmadas por un responsable y debidamente supervisadas.

En un entorno de administración electrónica, la entidad realizará las conciliaciones bancarias con un alto grado de automatización. Los movimientos bancarios (ficheros norma 43[7]) diarios se recibirán al día siguiente a través del sistema EDITRAN y se cargarán de forma automatizada en el sistema contable (ERP).

Una vez cargados estos movimientos, el ERP realiza un procedimiento de conciliación automatizado con los movimientos contables transitorios o provisionales. Cuando son coincidentes se contabilizan de forma automatizada en la cuenta contable de tesorería correspondiente.

Si hay movimientos no coincidentes quedan registrados como movimientos transitorios pendientes de investigación hasta que definitivamente se aclaran, concilian y contabilizan.

Las conciliaciones bancarias no deben arrastrar partidas de forma indefinida. Aunque con carácter general no puede fijarse un plazo para su aclaración, debe efectuarse de forma diligente y sin demoras no justificadas ni razonables.

- Controles sobre los **pagos**:
  - El sistema realiza de forma automática un cruce entre orden de pago, pedido y factura, identificando y bloqueando partidas no coincidentes.
  - El sistema impide el registro de facturas duplicadas.
  - El sistema bloquea pagos donde el importe total facturado supera el límite establecido en los pliegos y/o contratos.
  - El sistema verifica automáticamente que una factura u obligación pendiente de pago no ha sido pagada anteriormente.
  - Las órdenes de pago se revisan junto con la documentación de respaldo para verificar su idoneidad y precisión antes de aprobarlas.
  - Una vez aprobada la orden de pago nadie está autorizado a modificarla, excepto con la firma del Tesorero e Interventor.
  - El sistema bloquea la realización de pagos no presupuestarios si el importe a pagar es mayor al ingreso no presupuestario que da origen al pago.
  - Las firmas electrónicas en las órdenes de pago garantizan la integridad.
  - El ERP **impide** (por configuración) que se puedan realizar pagos a cuentas bancarias distintas de las del FMT. **No puede realizarse ningún pago** a un IBAN que no esté registrado en el FMT para el acreedor correspondiente, en caso contrario el pago es rechazado automáticamente por el ERP.
  - Las firmas electrónicas en los correos electrónicos de remisión de las órdenes de pago garantizan la identidad del remitente. Se aplica el protocolo DMARC (ver nota al pie nº 11 en el Anexo 1B).

[7] La norma 43 es un estándar bancario que regula y normaliza la transmisión de extractos bancarios de cuentas corrientes. Fue desarrollado por las entidades de crédito españolas a través de sus respectivas asociaciones, con especial participación de la Asociación Española de Banca (AEB). Sirve, en mayor medida, para facilitar un proceso contable tan crítico e importante como es la conciliación bancaria, es decir, el contraste de la información de las cuentas bancarias de una empresa con su contabilidad, a fin de detectar cargos o abonos pendientes y, en general, conocer el estado real de su tesorería.

Las entidades bancarias suelen enviar de manera diaria estos ficheros a las empresas que tengan contratado este servicio a través de redes P2P, generalmente a primera hora de la mañana. Una vez recibido, los sistemas empresariales integran todos estos movimientos en sus sistemas y ejecutan la conciliación bancaria de manera automática. Adicionalmente, las entidades permiten la descarga manual de esta norma.

Desde el punto de vista técnico, el cuaderno 43 (norma 43) es un fichero que tiene una estructura definida donde están reflejados todos y cada uno de los movimientos (cargos y abonos) de las cuentas bancarias de una empresa durante un intervalo de tiempo determinado. A pesar de que cada entidad puede estructurar este fichero de forma diferente, en la mayoría de los casos consta de varios tipos de registros: saldo inicial, movimientos y saldo final.

- Controles sobre las **interfaces**:
  - El acceso a la ruta donde se almacena la información que vuelca entre sistemas se encuentra debidamente restringido.
  - El ERP genera automáticamente los ficheros con el detalle de las transferencias bancarias en formato XML (Cuaderno 34) y lo remite al banco mediante un servicio web o canal seguro.
  - Cuando la interfaz no es automatizada, por ejemplo, si el fichero XML (Cuaderno 34) se envía a través de la página web de la banca electrónica, las carpetas donde se depositan los ficheros de pago están debidamente protegidos.
  - Una vez generado el fichero XML, la aplicación bloquea la orden de pago correspondiente.
- Controles sobre la **caja**
  - Existen procedimientos por escrito y aprobados para la gestión de las cajas de efectivo.
  - Se realiza un arqueo diario de los saldos de cada una de las cajas de efectivo llevando el control de entradas y salidas desde el saldo anterior. El arqueo es presenciado por un responsable que supervisa al cajero. El arqueo debe firmarse por ambos. En algunas ocasiones debe ser sorpresivo.
  - Existe una aplicación para registrar los ingresos por los precios públicos. Los usuarios de la aplicación pueden registrar, pero no borrar los apuntes de cobro. Los ingresos se traspasan automatizadamente a la contabilidad.
  - Sólo gestionan las cajas las personas que tienen asignadas estas tareas. Existe segregación de funciones respecto a contabilización y cobro.
  - El efectivo en caja está sometidos a eficaces procedimientos de custodia y protección física.
  - Debe haber protección contra los incendios, robos, etc. Existen cajas fuertes para proteger el efectivo.
- **Controles contables:**
  - La contabilización es automática.
  - Todos los asientos de tesorería no automatizados están restringidos y son supervisados.
  - El personal con acceso a modificar la información contable se encuentra adecuadamente restringido mediante la asignación de permisos de acceso a los menús de contabilización (mosaicos) en el ERP solo a los usuarios que lo requieren en base a las tareas asignadas. Las autorizaciones han sido proporcionadas en base a la aplicación del principio de mínimo privilegio, mitigando el riesgo de que se produzcan accesos no autorizados y se realicen contabilizaciones erróneas.
  - Todas las operaciones se acumulan, clasifican y resumen correctamente en las cuentas; los saldos contables se concilian periódicamente con los de los extractos bancarios.
- **Controles sobre el fichero maestro de terceros (FMT)**:
  - Existe un procedimiento aprobado que regula la tramitación de las altas y modificaciones del FMT. Todos los cambios en el FMT se realizan según este procedimiento, que incluye una adecuada segregación de funciones y la asignación de autorizaciones y responsabilidades en las distintas etapas del proceso.
  - Cualquier cambio en los datos del IBAN donde se realizan pagos debe estar justificado mediante un certificado de titularidad real o preferentemente mediante el servicio **Iberpay** integrado con el ERP.
  - Si la cuenta que aparece en la factura electrónica no coincide con la que conste en el FMT, no se pagará (nunca se debe pagar una factura a un IBAN que no conste en el FMT), se investigará, y en su caso, se requerirá al acreedor para que actualice sus datos a través del procedimiento electrónico.
  - En ocasiones los procedimientos de las entidades auditadas contemplan declaraciones responsables para acreditar la titularidad de las cuentas en el alta terceros y cuentas bancarias en el FMT. Este tipo de requisito o control, aunque es legal (art. 69 Ley 39/2015), no es un control tan robusto y fiable como los certificados o verificaciones mediante servicios web (tipo Iberpay).

- Los cambios en el FMT (nuevos proveedores, cambios de IBAN, ...) se procesan solo después de que se hayan obtenido las aprobaciones adecuadas, de acuerdo con el principio de mínimo privilegio.
- Los usuarios con capacidad para realizar cambios en el FMT se encuentran debidamente autorizados y restringidos de acuerdo con el principio de mínimo privilegio.
- Analizar si existe una adecuada SdF para llevar a cabo las altas y cambios del FMT y su aprobación. Tendremos en consideración el tamaño de la entidad y las disponibilidades de personal.
- Los controles de acceso al ERP (módulo FMT) están bien configurados.
- Los CGTI *D.1 Uso controlado de privilegios de administración* y *D.2 Gestión de usuarios* funcionan eficazmente, bajo el principio de mínimo privilegio.

Ver más información sobre estos controles sobre el FMT en el Anexo 1A.

- 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 **que sean relevantes o significativos** 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 de la tesorería.

Entorno de control

Un entorno de control efectivo es fundamental para asegurar que la información sobre la tesorería 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
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. Un elemento esencial en cualquier sistema de control interno es el denominado tono directivo. Es la forma en que la alta dirección expresa sus convicciones respecto de la importancia del control interno y determina en gran medida su eficacia.	**Alto** Debido a las circunstancias indicadas no se puede tener la seguridad de que todos los pagos 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.	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.

Un elemento clave del entorno de control es la existencia de una adecuada gobernanza de la ciberseguridad (véase GPF-OCEX 5314).

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 los cobros y pagos o los movimientos bancarios. Contemplará entre otras cuestiones que:

- Todas las solicitudes de cambios a introducir en las aplicaciones de gestión de tesorería, 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 SdF 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 de tesorería.

  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 de tesorería 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 tesorería. En concreto, se han identificado un total de 30 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.	**Alto** 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, incluyendo el riesgo de fraude.	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. Recomendamos que se apruebe formalmente un procedimiento para la gestión continua de cambios, que especifique los siguientes requisitos: - Registro de todas las solicitudes de cambio, incluidas las urgentes y las originadas desde el equipo técnico o desde los responsables funcionales del servicio. - Evaluación de las solicitudes teniendo en cuenta los riesgos de seguridad. - Autorización de los cambios por parte del personal responsable, previamente a su pase a producción. - Realización de pruebas, con carácter previo a la implantación del cambio y aceptación por parte del usuario final y de los responsables funcionales. - Planificación de la puesta en funcionamiento del cambio. - Mejorar la gestión documental del proceso e incluir toda la información necesaria.

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 tesorería y contabilidad están adecuadamente protegidas para evitar el uso no autorizado, divulgación, modificación o pérdida de información o la sustracción 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.

Solamente deben estar activos los usuarios estrictamente necesarios para desarrollar las funciones.

Privilegios elevados

El acceso o la modificación de los privilegios de acceso debe ser aprobado y documentado, 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. Este acceso "privilegiado" debe estar limitado estrictamente a las necesidades de la entidad.

Autenticación

Los usuarios del sistema de gestión de tesorería deberán ser identificados de forma única. Los usuarios tendrán un identificador individual de acceso y no deberán compartir contraseñas. Es muy importante 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
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, 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.	**Alto** 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.	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, HPUX, Directorio activo). Implantar el DFA.
Los permisos de administración del entorno SAP no se habían restringido suficientemente, existiendo un elevado número de usuarios con capacidad total sobre el sistema (perfil SAP_ALL). En el análisis efectuado se han detectado usuarios de gestión, proveedores externos, y usuarios que han causado baja en la Entidad, que disponen de permisos de administración. El perfil SAP_ALL básicamente consta de todas las autorizaciones posibles en SAP con lo cual, el usuario que tenga este perfil asignado puede realizar cualquier actividad sobre el sistema (tanto a nivel de sistema como a nivel de negocio, por ejemplo, crear usuarios, eliminar o modificar bases de datos, borrar o modificar registros, crear y autorizar órdenes de compra, etc.)	**Alto** La ausencia de control sobre los permisos de administrador de SAP otorgados a los usuarios durante el ejercicio representaba un alto riesgo por la posibilidad de acceso total a los datos, a la gestión económica y a la manipulación de los sistemas de información de la Entidad, con el perjuicio que podría ocasionarle. En dichos usuarios no existe el control basado en la segregación de funciones incompatibles.	Se recomienda mejorar la gestión de los usuarios administradores del entorno SAP. El perfil SAP_ALL debería ser asignado a un grupo muy reducido de usuarios, un máximo de dos o tres administradores de sistemas. Además, dicha asignación debería ir acompañada de unas políticas de seguridad adecuadas, como por ejemplo cambio periódico de contraseñas, registros de auditoría y revisiones periódicas de estas. Además, dicho perfil no debería ser asignado en ningún caso a: - Usuarios de negocio - Usuarios desarrolladores - Usuarios externos
Se han identificado 24 cuentas de usuario genéricas (lo que supone un 20% sobre el total de cuentas de usuario activas) cuyo uso no está justificado o bien no se conoce quién y para qué se utilizan.	**Alto** La utilización de cuentas genéricas impide mantener la trazabilidad de las acciones realizadas.	Realizar una revisión detallada de los usuarios existentes en la aplicación de gestión de Tesorería, 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.

Deficiencia de control observada	Riesgo	Recomendación
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.	**Medio** Esta situación implica un riesgo medio de accesos indebidos y de actuaciones no autorizadas.	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. También debe incluir la revisión periódica de los usuarios autorizados y sus privilegios 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.

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.
- Deben realizarse pruebas de restauración programadas.
- Hay que definir los plazos de retención y los requisitos de almacenamiento para la información.

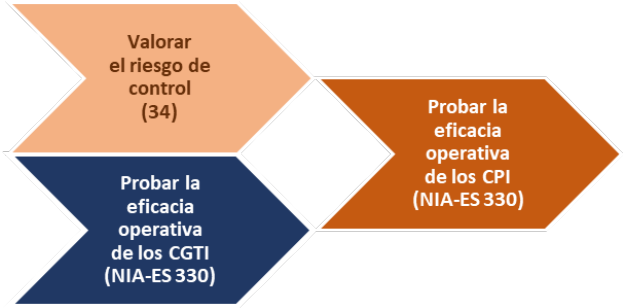
En el caso de que las aplicaciones informáticas de gestión de tesorería o parte de los sistemas de información utilizados se hayan contratado en modo Cloud (SaaS, PaaS o IaaS) deberán considerase las especificidades de los controles de TI en este entorno.

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 afecte al CPD, existe el riesgo **alto** 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 desarrollar un plan de recuperación ante desastres, que permita 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.
No se ha definido un plan de continuidad de la actividad que permita la recuperación de los procesos de gestión críticos en un tiempo limitado y fijado con anterioridad, tras la ocurrencia de una contingencia que afecte a los sistemas de producción.	Existe un riesgo **alto**, 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 Continuidad de la Actividad** corporativo, que incluya el análisis sobre elementos críticos de negocio existente, la estrategia de continuidad, los planes particulares de contingencia de los sistemas del Ayuntamiento y la ejecución planificada de pruebas periódicas del plan.
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 **alto** 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.

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[8].

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 para alcanzar ambos objetivos simultáneamente. 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 (SdF)

Al revisar el proceso de gestión de la tesorería, un aspecto fundamental es el estudio de la segregación de funciones, 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.

Debido a que, de todos los activos, el efectivo es el más susceptible de apropiación indebida, es especialmente

[8] Apartado A180 de la NIA-ES 315R/GPF-OCEX 1315R.

importante que se segreguen las funciones para que ninguna persona controle todas las etapas de gestión de la tesorería.

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 a 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 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**[9].

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 e indagar si existen controles compensatorios que mitiguen esos riesgos.

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.

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. Dada su complejidad y "no visibilidad" ese análisis 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 situaciones de conflicto de segregación de funciones en el proceso de gestión de tesorería, que pueden entrañar riesgos de errores o irregularidades, y por tanto riesgos de auditoría. Este cuadro solo es 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, ya que las funciones principales y, en consecuencia, sus conflictos, dependen de cada caso específico.

El procedimiento de auditoría lógico consistiría en describir los procedimientos de gestión de cobros y pagos, documentar las respuestas, la evidencia obtenida sobre los posibles conflictos de segregación de funciones 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
1	Tesorería	El empleado que formula las peticiones para abrir cuentas bancarias ¿puede autorizar dichas peticiones en el banco?	Existe un procedimiento aprobado para la apertura de cuentas bancarias que contempla la autorización de dos o más personas, incluyendo la que tiene la competencia para la contratación de este tipo de servicios.
2	Tesorería	¿Existen procedimientos aprobados para verificar que están controladas y registradas todas las cuentas bancarias a nombre de la entidad?	Existe un procedimiento aprobado que contempla la revisión periódica de las cuentas de la Entidad, e incluye la solicitud a la entidad bancaria para que envíe confirmación de las nuevas cuentas al departamento de tesorería, así como a un miembro del personal de la alta dirección distinto del autorizado.

[9] 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
			El personal encargado de la gestión y tramitación de la apertura de cuentas bancarias no puede contabilizar transacciones bancarias ni preparar las conciliaciones.
3	Tesorería	¿Las responsabilidades por la entrada y salida de efectivo están segregadas de todas las demás funciones conexas? *La SdF entre el registro de cobros y pagos, por una parte, y su contabilización, por otra, permite una revisión independiente de las operaciones de caja y para mantener la integridad de las cuentas de control del mayor general.*	Los empleados con responsabilidad por las entradas y salidas de efectivo deben ser independientes de las correspondientes funciones de gestión y contabilidad (como expedición, facturación, notas de abono, cuentas por cobrar, compras, cuentas por pagar y nómina).
4	Tesorería	¿La responsabilidad de los cobros en efectivo está segregada de la correspondiente a los pagos en efectivo? *La mezcla de las actividades de cobros y pagos puede dar oportunidad de ocultar apropiaciones indebidas de cobros mediante la manipulación del proceso o del registro de los pagos. P.e., puede desviarse el importe recibido de una cuenta a cobrar sin afectar el saldo de la cuenta de caja si la anotación del ingreso desviado se compensa con la anotación de un desembolso simulado por el mismo importe.*	Ningún empleado puede simultanear dichas tareas.
5	Conciliaciones bancarias	El empleado responsable de preparar las conciliaciones bancarias ¿realiza también alguna de las siguientes tareas? • Recibir las entradas de caja/cobros por caja • Preparar los depósitos de caja • Preparar o autorizar transferencias • Ejecutar o autorizar transferencias bancarias • Revisar y aprobar la conciliación bancaria • Contabilizar operaciones bancarias	La persona que prepara las conciliaciones no debe encargarse de registrar los cobros o pagos, ni contabilizar operaciones de tesorería. *Las malversaciones de efectivo pueden ocultarse falseando las conciliaciones.* *Si la responsabilidad por la preparación y aprobación de las conciliaciones se asigna a personas independientes de las actividades de proceso y registro de tesorería, no sólo hay menos oportunidad de realizar manipulaciones, sino que también se instrumenta un medio para descubrir los errores en el proceso o registro tanto de cobros y pagos.*
6	Conciliaciones bancarias	¿Son supervisadas las conciliaciones bancarias?	Las conciliaciones deben ser revisadas y aprobadas por una persona distinta de la que las ha preparado.
7	Cobros	¿El empleado responsable de cobros en efectivo también lleva a cabo alguna de las siguientes funciones?: • Contabilizar los cobros • Registrar o autorizar saneamientos o ajustes en las cuentas de deudores en contabilidad • Conciliar las cuentas bancarias	El empleado responsable de recibir el efectivo no debe tener acceso a registrar o autorizar operaciones en contabilidad. La persona que recibe el dinero en efectivo o que prepara su depósito en bancos no debería ser responsable de registrar las transacciones en metálico ni tampoco preparar las conciliaciones bancarias. *Se deben implantar procedimientos para minimizar los cobros en efectivo. Si se realizan deben ser supervisados por persona distinta de quien los realiza.* *Deben realizarse arqueos diarios o semanales de los cobros y pagos en efectivo que deben firmarse por la persona que gestiona los fondos y por la que lo revisa.*
8	Mantenimiento del Fichero Maestro de	El empleado responsable del mantenimiento del FMT (p. ej. añadir, borrar o cambiar/modificar las	El empleado con responsabilidad para modificar/introducir cambios en el FMT no debe ser responsable de introducir las facturas de acreedores en

#	Función	Consideraciones de control / Preguntas de auditoría	Controles posibles/ Recomendaciones
	Terceros (FMT)	cuentas bancarias de acreedores) ¿realiza también alguna de las siguientes tareas/funciones?: • Contabilizar o modificar los asientos y/o documentos de contabilización de las obligaciones o de los pagos. • Aprobar las facturas de acreedores • Realizar o autorizar transferencias	el sistema contable ni tampoco tener capacidad para efectuar y autorizar pagos.
9	Mantenimiento del FMT	Los cambios en el FMT (p.ej. cambios en las direcciones o nombres de terceros y altas en el FMT), ¿son revisados y aprobados por un supervisor de quien los introduce?	Las altas o modificaciones del FMT deben ser revisadas o fiscalizadas previamente a estar disponibles para su uso en el sistema contable. Se emite un informe sobre los cambios en el FMT que es revisado por un empleado que no tenga acceso o responsabilidad para realizar esas funciones.
10	Pagos	Los empleados responsables de aprobar las facturas y los pagos ¿pueden también contabilizar en proveedores? *Si quienes tramitan o aprueban los pagos controlan también su contabilización, hay mayor oportunidad de que se efectúen pagos no autorizados o respaldados por documentos simulados y de que se registren luego las operaciones en cuentas no sujetas a un control riguroso.*	Los empleados responsables de autorizar las facturas y pagos a los acreedores no deberían encargarse de contabilizar las facturas.
11	Pagos	¿La disposición de fondos es mancomunada? ¿Es la transferencia el medio normal de pago	Las disposiciones de fondos de cuentas bancarias se realizan de forma mancomunada y el medio normal de pago es la transferencia bancaria.
12	Pagos	La persona responsable de autorizar transferencias bancarias ¿realiza también alguna de las siguientes funciones? • Preparar las transferencias • Preparar las conciliaciones bancarias • Revisar y aprobar las conciliaciones bancarias • Contabilizar facturas de proveedores • Introducir cambios en el FMT • Aprobar las facturas y los documentos OK • Gestión de compras y proveedores	La preparación y la aprobación de transferencias bancarias deberían ser realizados por dos empleados distintos. El empleado responsable de autorizar las transferencias a los proveedores no debe tener competencia para introducir cambios en el FMT, contabilizar las facturas de proveedores ni tampoco participar en el proceso de conciliación bancaria. Se revisan los pagos a realizar por personal diferente del de tesorería previamente a la realización del pago. Los pagos realizados son verificados a posteriori por personas diferentes de los que los tramitan.

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)*

Las interfaces son programas que sirven para transferir datos de una aplicación a otra. Las entidades pueden utilizar sistemas de gestión de tesorería distintos de los sistemas contables y aplicaciones de gestión de otros procesos que comparten la información mediante interfaces.

Las interfaces hacia y desde el sistema de cobros/pagos/tesorería presentan un área de riesgos significativos para el mantenimiento de la integridad de los datos.

Por ejemplo, un caso común es aquel en que una entidad envía a los bancos, mediante una interfaz, los datos de las transferencias (pagos) a realizar. Esa interfaz externa (mediante la que se remite a las entidades financieras el fichero de pagos en formato XML) es un foco de riesgo de fraude de apropiación indebida si no está

debidamente protegida frente a accesos indebidos (El acceso a los ficheros bancarios para pagos debe estar restringido al personal que lo necesite de acuerdo con sus funciones).

Además de la interfaz de pagos con el banco, se debe prestar atención a las que interactúan con otras aplicaciones, como la de contabilidad o la de recaudación, etc.

Las interfaces pueden estar automatizadas o ser manuales. En ambos 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:

a) Identificar las interfaces existentes que puedan afectar significativamente a las cuentas anuales y suponer un riesgo de auditoría.

b) Identificar y evaluar los controles que tenga establecidos la entidad para garantizar la exactitud e integridad de los datos traspasados.

c) Diseñar y ejecutar las pruebas de auditoría que se estimen pertinentes sobre las interfaces para garantizar la exactitud e integridad de los datos.

14. Revisión del cumplimiento legal

El objetivo de la fiscalización de cumplimiento consiste en verificar que la organización y gestión de la tesorería es conforme y se realiza de acuerdo con la normativa aplicable.

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

Es aplicable la guía GPF-OCEX 4320.

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 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 en base a la valoración del riesgo de incorreciones materiales, e incluirán:

- Pruebas de controles (si procede).
- 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.

Algunos de los principales **procedimientos sustantivos** son:

- Obtener confirmaciones bancarias.
- Realizar arqueos de caja (cuando sea significativa) y conciliar con la contabilidad.

En el Anexo 2 se incluye, a modo de ejemplo, un programa de auditoría que debe ser adaptado a las circunstancias de cada fiscalización.

Pruebas masivas de datos

La utilización de aplicaciones informáticas para la gestión de la tesorería y su contabilización permite realizar pruebas masivas de datos para verificar su adecuada gestión. 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 de tesorería 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, …
- Analizar los usuarios autorizados para acceder a la aplicación de gestión de tesorería o perfiles de tesorería de la aplicación de contabilidad. Seleccionar usuarios administradores (todos o una muestra, en función del número) para comprobar que están autorizados.
- Verificar el correcto funcionamiento de la interfaz entre la aplicación de tesorería y la de contabilidad.
- Revisar las conciliaciones bancarias.
- Revisar las interfaces de pagos. Verificar que la aplicación genera correctamente los ficheros de pagos xml (C34).
- Verificar, en su caso, la interfaz de entrada automatizada de los movimientos de las cuentas bancarias en contabilidad (C43).

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.

Documentación del conocimiento del proceso de gestión de tesorería

El auditor debe describir y documentar el conocimiento del proceso de gestión de tesorería de la Entidad.

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

- **Qué** transacciones y operaciones se realizan en el proceso: Contratación y baja de cuentas bancarias, ingresos, pagos, órdenes de pago, registro contable de los ingresos y pagos, fiscalización formal y material del pago, conciliaciones, registro de terceros, fiscalización alta terceros, …
- **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 diagrama de flujo, 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.

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

Los párrafos sombreados en amarillo incluyen información adicional y ejemplos que se puede considerar al hacer la descripción del proceso, pero que se debe eliminar del documento final, ya que solo tiene valor informativo para el auditor que está documentando el proceso.

##########

Entidad: _____

Fecha CCAA: _____

Resumen realizado por (Técnico/fecha): _____

Revisado por (Auditor/fecha): _____

Persona/s entrevistada/s: _____

1. Aspectos generales y organizativos

Se debe indagar y preguntar a los responsables de la gestión de tesorería cuestiones como:

- Solicitar/obtener el organigrama de la entidad que incluya el departamento de tesorería. ¿Está aprobado?

  Si no existe, realizar uno en base a la información obtenida tras cumplimentar este anexo 1.

- ¿El departamento de tesorería es independiente de cualquier otro de la entidad?

  Sí / No

- ¿Hay normas o procedimientos escritos sobre la gestión de la tesorería?

  Sí (adjuntar) / No

- ¿Están claramente definidas las responsabilidades de cada empleado? ¿Estas funciones y responsabilidades están expuestas por escrito?

  Sí / No

- ¿Son suficientes los efectivos existentes para cubrir las necesidades del servicio?
- ¿Existen medios para asegurar que el personal cuenta con los conocimientos y/o formación necesarios para realizar su trabajo? ¿Se realizan actuaciones de formación para mantener/actualizar estos conocimientos? ¿Con qué frecuencia?
- ¿Existe la debida segregación de funciones dentro de este departamento? (Ver apartado 12 de la guía).

  Sí / No
- El personal de tesorería realiza, en algún caso, funciones de:

  ¿Registro de cuentas a cobrar?
  ¿Decisión sobre descuentos, bonificaciones, etc…, en ingresos?
  ¿Preparación de documentos de pago y nóminas?
  ¿Registro contable de caja o bancos?
  ¿Preparación de facturas de venta y registro contable de las mismas?
  ¿Conciliaciones bancarias?
- ¿Existe una política sobre el manejo de fondos clara y definida?

  Sí / No
- ¿Tiene la entidad problemas de cash-flow de tesorería para hacer frente puntualmente a sus obligaciones de pago?
- ¿Utiliza la entidad programas de gestión de tesorería de forma efectiva?
- La entidad utiliza las siguientes aplicaciones informáticas:

  Gestión de tesorería:

  Contabilidad: SAP / SicalWin / Desarrollo propio /….
- ¿Utiliza la entidad algún servicio de gestión de tesorería ofrecido por las entidades financieras? ¿De qué tipo? ¿Banca electrónica? ¿quién tiene acceso a la banca electrónica, con qué funcionalidades? Detallar.
- ¿Ha realizado la entidad algún cambio significativo en sus procedimientos de tesorería en el último año?

  ¿Y en el sistema informático?

  ¿Y en la normativa?

  ¿Y en el personal clave?
- ¿Realiza el departamento de control interno revisiones periódicas?
- ¿Se ha realizado algún tipo de actuación de control por otro órgano?
  Si sí, solicitar informe de resultados.
- ¿Tiene el equipo de auditoría algún motivo para sospechar que la dirección puede tener algún interés en manipular los saldos de tesorería?

2. Flujograma general (resumido) y detallado

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

3. Gestión de la tesorería

En las EELL revisar las bases de ejecución del presupuesto.

El auditor debe describir:

a) Las operaciones de gestión de tesorería se inician de la siguiente forma:

b) Las operaciones de gestión de tesorería se autorizan de la siguiente forma:

c) Las operaciones de gestión de tesorería se registran de la siguiente forma:

d) Las operaciones de gestión de tesorería se procesan y se reportan en los estados financieros de la siguiente forma:

4. Bancos

Objetivo de control: Todos los saldos en cuentas bancarias están sometidos a eficaces procedimientos de control

La apertura de cuentas solo puede realizarse por personas con poder suficiente.

¿Están debidamente autorizadas las cuentas bancarias y las personas que firman las disposiciones?

¿Es **mancomunada** la disposición de efectivo?

Sí / No

¿Qué personas están autorizadas para disponer de las cuentas bancarias?

¿Se avisa a los bancos cuando un firmante autorizado deja de serlo?

Se deben implantar procedimientos para notificar inmediatamente a los bancos cada vez que una persona autorizada para disponer de fondos deje de formar parte de la empresa.

¿Se tiene constancia de la recepción de dicho aviso?

Solicitar el inventario de cuentas al tesorero/responsable de tesorería y hacer un resumen de las cuentas bancarias utilizadas:

Denominación de la cuenta	Finalidad de la cuenta	Tipo de cuenta	Entidad financiera	Número de cuenta	Libre disposición/ Con restricciones	Saldo a 31/12/24	Firmas autorizadas durante 2024	Altas de firmas en 2024	Bajas de firmas en 2024	Tipo de disposición (solidaria, mancomunada)

5. Conciliaciones bancarias

Objetivo de control: Todas las operaciones se acumulan, clasifican y resumen correctamente en las cuentas; los saldos de contabilidad se concilian con los de los extractos bancarios.

Las conciliaciones bancarias, incluso cuando las realizan personas independientes de las funciones relacionadas con el efectivo, no siempre ponen de manifiesto la existencia de operaciones irregulares; sin embargo, reducen la oportunidad de ocultarlas.

¿Se concilian periódicamente las cuentas bancarias?

Sí / No

¿Con qué periodicidad?

Diaria/Semanal/Mensual

¿Son automáticas o manuales?

¿Quién las realiza y quién las revisa?

Los procedimientos manuales para realizar las conciliaciones bancarias de todas las cuentas, ¿incluyen?:

a) La recepción de los extractos bancarios directamente por la persona encargada de las conciliaciones.

b) La comparación de las fechas e importes de los depósitos en bancos, tal y como se indican en el extracto, con el libro mayor.

   No deben existir diferencias que pudieran indicar que los fondos han sido utilizados para otros fines durante el periodo previo a su depósito en el banco.

c) La investigación de las transferencias interbancarias, para comprobar si ambas partes de la transacción han sido debidamente contabilizadas.

   Hay que verificar si las transferencias han sido registradas en el mismo período contable en los dos bancos.

d) La revisión de las conciliaciones bancarias por una persona responsable.

   La mera realización de una prueba aritmética entre el saldo según libros y el extracto es insuficiente. Se debe realizar un cuidadoso examen de todas las partidas de la reconciliación y se debe obtener una explicación satisfactoria para todas ellas.

Si son manuales ¿se realizan y revisan o aprueban por personal ajeno al departamento de tesorería?

Sí / No

¿O están automatizados? Describir el procedimiento.

¿Son adecuados los procedimientos de conciliación de las cuentas bancarias?

6. Caja

Objetivo de control: El efectivo en caja está sometido a eficaces procedimientos de custodia y a protección física

Consideraciones previas: La amplitud del conocimiento de los procedimientos, su descripción y la del control interno relacionado será proporcional a su significatividad. Si es poco significativo se reducirán los procedimientos para su conocimiento y su posterior revisión.

La entidad debe estar atenta a todo aumento del movimiento de los fondos de efectivo, ya que esto puede ser indicio de que se están utilizando en operaciones que deberían ser tramitadas a través de los procedimientos normales de pago. Un modo de reducir dicha actividad a un mínimo consiste en poner un límite al importe de los pagos realizados con fondos de la caja fija.

Los fondos de caja fija y otros fondos de maniobra deben ser administrados por el sistema de fondo fijo y por una persona que no desarrolle otras funciones relacionadas con el efectivo. Deben prepararse los justificantes o recibos de manera que hagan imposibles las alteraciones y los cheques de reposición de fondos deben extenderse a favor de la persona responsable de la custodia de los fondos.

No podrán pagarse en efectivo las operaciones, en las que alguna de las partes intervinientes actúe en calidad de empresario o profesional, con un importe igual o superior a 1.000 euros. (Artículo 18 de la Ley 11/2021 de 9 de julio).

¿Se realizan cobros o pagos por caja?

Sí / No

¿Cuál es el volumen gestionado por las cajas de efectivo al año? ¿Es significativo?

Identificar el número de cajas que dispone la entidad y quién es el responsable que autoriza su apertura

¿Existe algún límite de fondos en caja?

Describir los mecanismos de custodia de efectivo

¿Se realizan arqueos periódicos?

Deben realizarse arqueos de caja periódicos, sin previo aviso, por parte de una persona independiente de todas las demás funciones relacionadas con el efectivo.

¿Quién los realiza?

¿Son adecuados los controles sobre los fondos de efectivo?

¿Es adecuada la protección física de los fondos de efectivo? ¿Se utiliza una caja fuerte para la custodia de los fondos de efectivo?

La adecuación de la protección física de los fondos de efectivo depende del grado de riesgo de pérdida por causa de incendio, negligencia o robo. La protección física puede comprender el uso de cubículos especiales para los cajeros, de cajas acorazadas con doble combinación, de sistemas de depósito de seguridad y de cajas ignífugas. También dependerá del volumen de los movimientos de fondos por caja.

¿Se usa el sistema de fondo fijo para todas las cajas?

El sistema de fondo fijo simplifica el control sobre los importes en caja, fijando el importe total por el cual el cajero es siempre responsable.

Uno de los principios del sistema es que el fondo sea reembolsado tan sólo bajo presentación de los justificantes de caja debidamente aprobados y por la suma de tales justificantes.

¿Se encuentra cada fondo fijo o cada caja bajo la responsabilidad de una persona únicamente?

Se trata de ver si la responsabilidad por cada fondo está total y claramente asignada a un individuo.

¿Está establecido el importe máximo de los pagos que pueden hacerse de cada fondo?

Los procedimientos deben hacer que todos los desembolsos importantes atraigan la atención de las personas responsables de su revisión y aprobación antes de que el pago sea realizado.

El fondo en efectivo tiene por objeto atender los pagos urgentes y de poco importe. Las prevenciones que se toman para los pagos por transferencia no se toman generalmente para los pagos efectuados por caja. Es aconsejable limitar los importes que pueden pagarse por caja bajo la exclusiva responsabilidad del cajero.

Los desembolsos por caja ¿están documentados por justificantes debidamente aprobados?

¿Se obliga, en todos los casos, a firmar los recibos a la persona que recibe el dinero?

Se debe tener especial cuidado cuando los comprobantes no están respaldados por una factura u otro documento indicativo del importe, preparado independientemente del comprobante.

¿Aprueban la reposición del fondo personas ajenas a su custodia, después de un examen minucioso de los comprobantes?

Quien firma un pago debe estar seguro de que el importe responde a unos cargos adecuados y que anteriormente no fueron pagados.

¿Se cancelan de forma efectiva los comprobantes a fin de evitar la repetición de su uso?

Los auditores internos u otros empleados responsables ¿practican arqueos de caja por sorpresa?

El fondo de caja debe siempre estar compuesto por efectivo o por comprobantes de los desembolsos efectuados. El fondo no debe utilizarse para anticipos no autorizados o desembolsos similares que constituyen un uso impropio de los fondos de la empresa (anticipos de fecha antigua).

7. Cobros

Objetivo de control: Todos los cobros se identifican correctamente, se obtienen los totales de control y se ingresan íntegros y rápidamente en bancos

¿Son adecuados los procedimientos para procesar e ingresar los pagos realizados por los clientes/ usuarios/ contribuyentes?

Todas las entradas de efectivo deberán ingresarse intactas y rápidamente.

Un control práctico y eficaz sobre las entradas de efectivo consiste en utilizar únicamente las transferencias bancarias o ingresos en cuentas restringidas como medio de cobro.

¿Son adecuados los procedimientos fijados para las entradas de efectivo?

Si el personal de algún departamento recibe efectivo directamente, puede ser necesario el uso de impresos de recibo prenumerados, de cajas registradoras con totales inalterables u otros procedimientos de control, dependiendo del volumen y del tipo de las operaciones implicadas.

Todas las entradas, junto con la documentación apropiada, deberán ser enviadas íntegras a la persona responsable de efectuar los ingresos en bancos. Una copia de la lista-resumen o del informe de los cobros deberá enviarse al departamento de contabilidad para su subsiguiente cotejo con los ingresos bancarios y su contabilización.

¿Qué tipos de ingresos diferentes obtiene la entidad?

¿En qué cuentas bancarias se depositan los ingresos a través de banco? ¿Existen cuentas restringidas de ingresos?

¿Se producen ingresos por caja? (En caso afirmativo describir el procedimiento hasta su ingreso en una cuenta bancaria).

¿Existen sistemas de cobro a través de tarjeta de crédito, domiciliaciones de recibos u otros similares? En caso afirmativo, identificar el circuito de cobros y la conciliación de los ingresos con las liquidaciones efectuadas por la entidad.

¿Qué aplicaciones de gestión de ingresos y cobros emplea la entidad?

El auditor debe describir:

a) Departamento/servicio que realiza esta función:

b) El proceso se inicia y desarrolla de la siguiente forma:

c) Persona responsable entrevistada:

d) Consideraciones sobre la Segregación de funciones

8. Pagos

Objetivo de control: ***Todos los pagos se preparan basándose en la documentación adecuada y aprobada; se comparan con los datos justificativos, se aprueban, y se ordenan según las normas establecidas***

Ver Anexo 1B.

¿Los pagos se realizan únicamente mediante transferencias bancarias?

¿Son adecuados los procedimientos de autorización de los pagos?

La ordenación de los pagos puede suponer la aprobación definitiva en el proceso de gastos. Si se realiza correctamente por personas conscientes y competentes, esta tarea es un control importante de las operaciones antes del desembolso.

En las entidades pequeñas, en las cuales el número limitado de empleados reduce las oportunidades de segregación de funciones (SdF), la aprobación final de los pagos por el director puede ser el único sustituto eficaz de los controles que se consiguen en las organizaciones mayores a través de la SdF.

Para que la aprobación final sea eficaz, se debe facilitar al ordenante de la transferencia documentación justificativa suficiente para:

(1) comprobar la necesidad del gasto realizado,

(2) determinar si la operación fue correctamente iniciada por un empleado autorizado,

(3) satisfacerse de que todas las fases del proceso de la operación se han llevado a cabo de acuerdo con la normativa / los procedimientos establecidos, y

(4) revisar si la imputación contable se ha realizado correctamente.

Si los firmantes de transferencias no dan importancia a la función de aprobación final, no sólo se produce una pérdida de control de las operaciones normales del negocio, sino que se puede abrir el camino para la realización de operaciones no autorizadas.

Los pagos se realizarán utilizando una aplicación de banca electrónica en una terminal segura. Se considerarán **controles** relevantes:

- El archivo (ISO 20022 XML) conteniendo los datos para realizar la transferencia bancaria se almacena en una carpeta segura de la red corporativa y se transmite de forma segura.
- La orden bancaria de pago debe requerir, al menos, dos firmas mancomunadas. Verificar si se utilizan firmas electrónicas que impiden o dificultan la falsificación de las órdenes de pago.

Un control manual importante es la conciliación entre el documento de transferencia bancaria y el resumen de los pagos por la persona que va a autorizar el pago.

Si las órdenes de pago se envían por correo electrónico a la entidad financiera se debe añadir la firma electrónica de la persona que envía al correo para evitar ataques de "man in the middle" que puedan falsificar los datos de los pagos. En caso de que no pueda implementarse este control se deberían establecer controles alternativos, como un procedimiento que garantice que la entidad bancaria comprueba telefónicamente el origen de los pagos enviados superiores a un determinado importe.

Analizar si están correctamente definidas las responsabilidades y verificaciones a realizar por la entidad financiera en el proceso de pago (requerir firma mancomunada, autenticar firmas autorizadas, requerir firma electrónica, reconciliación de totales e identificación de los ficheros de pago, …).

El auditor debe describir:

a) Departamento/servicio que realiza esta función:

b) El proceso de pago se inicia y realiza de la siguiente forma:

c) El proceso de pago es autorizado de la siguiente forma:

d) Las órdenes de pago se envían de la siguiente forma:

e) La entidad financiera realiza las siguientes verificaciones en cada envío de orden de pago:

f) Los pagos son contabilizados de la siguiente forma:

g) Los registros de pagos son reconciliados con los extractos bancarios y saldos de las cuentas de mayor de la siguiente forma:

h) Persona responsable entrevistada:

i) Consideraciones sobre la Segregación de funciones:

9. Pagos a justificar (PJ) y anticipos de caja fija (ACF)

¿Se han detectado incumplimientos legales en la expedición de órdenes de PJ y de ACF (inexistencia de Acuerdo/Resolución, superación de cantidades máximas, gastos imputables a conceptos presupuestarios no autorizados, etc.)?

¿Existe una adecuada calidad de las cuentas justificativas, que eviten una inadecuada utilización de los fondos?

¿Se produce una utilización abusiva del sistema de anticipos de caja fija, pagos a justificar o procedimientos equivalentes, con respecto al procedimiento ordinario de pago (pagos en firme)?

10. Contabilidad

Objetivo de control: Todas las operaciones se registran pronta y exactamente en contabilidad o en registros auxiliares y se emiten los informes apropiados

¿Aseguran los procedimientos empleados que los cobros y los pagos se registran prontamente?

La demora en la contabilización de las cantidades cobradas o de los pagos dará lugar a que los saldos de efectivo sean mayores o menores de lo que debían ser al final del período contable.

¿Si la aplicación contable es distinta de la de gestión de la tesorería, la interfaz entre ambas tiene controles que garanticen la integridad de la información traspasada?

¿Son adecuados los procedimientos para la autorización y el registro de las transferencias interbancarias?

Todas las transferencias deben ser ejecutadas por las personas autorizadas o, en el caso de las transferencias automáticas (p. e., desde el banco depositario al banco en que la empresa tiene centralizadas sus operaciones) habrán de ser amparadas por las normas y procedimientos establecidos.

Las técnicas contables utilizadas para registrar las transferencias interbancarias deben garantizar que tanto los reintegros como los ingresos se registran correcta y prontamente en el mismo período y en las dos cuentas afectadas por la transferencia.

11. Mantenimiento del fichero maestro de terceros (FMT): Alta o modificación de datos de terceros y de cuentas bancarias

Ver Anexo 1A

Describir el procedimiento para dar de alta a un tercero, indicando la documentación que se solicita al tercero para confirmar la titularidad de la cuenta. (Véase a continuación un ejemplo). Debe averiguarse:

¿La entidad mantiene un registro de terceros (FMT)?

¿El registro es informatizado?

¿Validan el IBAN con Iberpay?

¿Está conectado con la contabilidad?

¿Quiénes son los autorizados para introducir o modificar los datos de un tercero?

¿Con qué periodicidad se comprueban los datos de los terceros con los que opera la entidad?

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: ____

Anexo 1 A Consideraciones sobre el fichero maestro de terceros (FMT)

Los ficheros maestros contienen los datos permanentes utilizados por múltiples aplicaciones y participan en la correcta ejecución del procesamiento de datos realizados por las aplicaciones.

Para que cualquier acreedor pueda recibir un pago, es un requisito que figure en el **fichero maestro de terceros (FMT)** acreedores de la Entidad con sus datos identificativos, incluyendo la cuenta bancaria (**IBAN**) a la que se realizarán los pagos.

El mantenimiento de su integridad es un elemento crítico para la correcta ejecución de la aplicación de gestión de la tesorería y para controlar que solo se realicen pagos a terceros autorizados en sus cuentas bancarias verificadas.

Es necesario que la entidad tenga un procedimiento escrito, detallado, completo, claro y debidamente aprobado que abarque todas sus fases y deje claras las funciones y responsabilidades de todos los intervinientes.

1.1 Procedimiento electrónico alta o modificación de terceros

De acuerdo con el artículo 14.2 de la Ley 39/2015 de PACAP **el procedimiento ordinario de comunicación será electrónico**. En este procedimiento, los terceros deben acceder a la Sede Electrónica de la Entidad, dónde deben identificarse electrónicamente por cualquiera de los medios admitidos por el sistema Cl@ve del Gobierno Español (Cl@ave móvil, Certificado electrónico/DNI, Cl@ve PIN, o Cl@ve permanente) e iniciar el procedimiento.

Cuando se accede para realizar el trámite como representante, si no se está dado de alta en el registro electrónico de representantes, se debe aportar la documentación justificativa que acredite la representación.

Una vez dentro del trámite, los datos identificativos de la persona que accede se rellenan automáticamente y se deben añadir otros datos personales o de la cuenta bancaria que se quiere dar de alta o modificar. Se admiten cuentas de los países adheridos al sistema SEPA de cuentas bancarias europeas y también de fuera de este sistema bancario.

Se exige que la cuenta bancaria a añadir al registro sea de titularidad de la persona que realiza la solicitud o a quien se representa. Para acreditarlo, se exige un certificado de la entidad bancaria de titularidad de la cuenta, que deberá estar firmado digitalmente o con CSV (conjunto de dígitos que identifica de forma única los documentos electrónicos).

Las declaraciones responsables previstas en el artículo 69 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, utilizadas como justificantes de la titularidad de la cuenta bancaria, aunque son un procedimiento legalmente previsto, no constituyen un control robusto a efectos de garantizar efectivamente la titularidad de la cuenta bancaria. En los apartados siguientes se describen procedimientos automatizados para verificar esta titularidad con garantías adecuadas.

Una vez presentada la documentación y grabada directamente la información por el interesado se fiscaliza en Intervención, que, previamente al alta del tercero, revisa que toda la información es correcta y está debidamente acreditada. En este momento todos los datos de la solicitud se cargan automáticamente en el FMT.

1.2 Procedimiento presencial de alta o modificación de terceros no obligados a comunicarse electrónicamente

En el procedimiento presencial de alta o modificación de terceros no obligados a comunicarse electrónicamente los solicitantes deben de personarse en el Registro general del Ayuntamiento o en cualquiera de las oficinas habilitadas para ello.

En estas sedes se debe presentar la solicitud mediante un formulario que se puede descargar de la Web del Ayuntamiento, en la que consignan sus datos personales y de la cuenta bancaria a registrar.

Los requisitos documentales para acreditar la titularidad de la cuenta bancaria son los mismos que en el trámite electrónico. Sin embargo, en esta forma de tramitación se debe presentar también, en todo caso, acreditación de la identidad persona solicitante y/o de la persona representada mediante la aportación de su documento de identificación fiscal completo.

La documentación presentada en papel se digitaliza para continuar el resto de la tramitación de forma electrónica.

El resto de los requisitos son los mismos que en el trámite electrónico.

1.3 Verificación del IBAN hasta el 9 de octubre de 2025

Un aspecto importante en el mantenimiento del FMT es la verificación de la concordancia del titular real del IBAN con el acreedor o tercero que consta en el FMT. La certificación de la entidad financiera da una cierta seguridad, pero se han cometido fraudes en los que se ha falsificado esa certificación. Recientemente se ha implantado el servicio de verificación **IBERPAY** que da solución a esta problemática.

¿Qué es el servicio de titularidad de cuentas Iberpay?
Fuente: https://www.iberpay.com/es/servicios/sectoriales/titularidad-de-cuentas/

El servicio de titularidad de cuentas es un servicio sectorial, digital y de alto valor añadido, prestado por Iberpay, que permite la verificación instantánea de la titularidad de las cuentas bancarias españolas en tiempo real y 24x7.

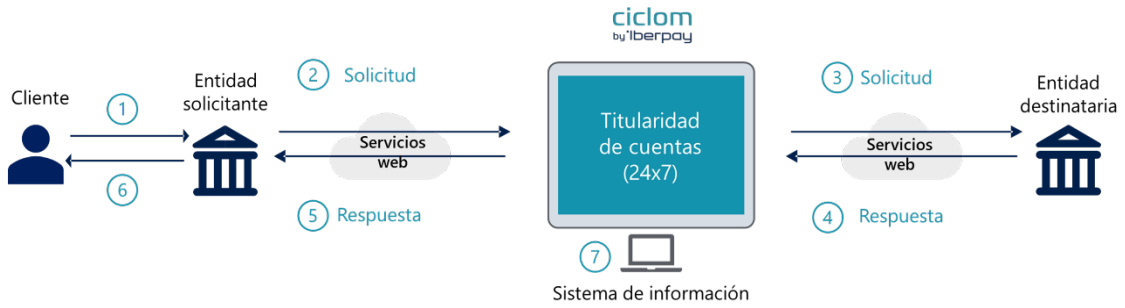
Desarrollado por Iberpay, este servicio cuenta con la participación de todas las entidades del sistema bancario español, lo que permite confirmar la titularidad de más de 80 millones de cuentas de pago (el 99% de las cuentas bancarias españolas).

Titularidad de cuentas es un servicio digital que ayuda a **reducir el fraude en los pagos** de cuenta a cuenta y a **reducir errores** en las transacciones comerciales, los pagos y los cobros. Además, facilita que la propia operativa bancaria se vea significativamente mejorada, dado que el banco reduce la operativa fraudulenta y errónea que recibe de sus clientes, evita excepciones y procesos manuales, y mejora el proceso automático “end-to-end” de los pagos.

Las claves del servicio:

- Confirmación de la titularidad de cualquier cuenta de pago, CIF/NIF contra el código IBAN de una cuenta, a través de un **servicio digital, instantáneo y 24x7**.
- **Evita fraude**: verifica la cuenta del beneficiario en tiempo real, por ejemplo, antes de enviar pagos o cobros, o en el proceso de onboarding digital de clientes.
- **Reduce errores:** anualmente, se registran +5 millones de devoluciones y más de 0,38 millones de rechazos de operaciones de pago.
- **Certifica la titularidad**: sustituye al certificado de titularidad bancaria de forma digital.
- **Información fidedigna,** más actualizada, en tiempo real.
- **Universalidad y sin fricción**: +80 millones de cuentas verificables en España (≈ todas), sin fricción y en menos de tres segundos.
- Comercialización y acceso al servicio **a través de los bancos**.

¿Cómo funciona el servicio Iberpay?



Paso 1-**Inicio de la solicitud:** el proceso comienza cuando un cliente bancario solicita a su entidad la confirmación de la titularidad de una cuenta.

Paso 2-**Solicitud de verificación:** la entidad inicia la solicitud con los detalles de titularidad de una cuenta que se desea verificar.

Paso 3-**Verificación en tiempo real:** Iberpay utiliza su tecnología en tiempo real para remitir dicha solicitud a la entidad confirmante de cuyo cliente se desea confirmar la titularidad.

Paso 4-**Confirmación de la titularidad:** la entidad confirma si los datos proporcionados son correctos y proporciona una respuesta inmediata sobre la autenticidad de la cuenta.

Paso 5-**Resultados de la verificación**: los resultados de la verificación se envían de vuelta a la entidad solicitante. Este proceso tarda menos de un segundo.

Paso 6-**Uso en transacciones o procesos comerciales**: con la información de la titularidad confirmada en tiempo real, la empresa o cliente puede proceder con confianza en sus operaciones financieras o comerciales, evitando fraudes y errores relacionados con la titularidad de la cuenta.

Iberpay se integra en el ERP de la entidad auditada y se comunica automáticamente vía servicios web con las entidades financieras por lo que al autorizar el alta del IBAN en el FMT, Tesorería puede hacer, con carácter previo, esta comprobación de forma automatizada.

1.4 Verificación del IBAN/beneficiario después del 9 de octubre de 2025

El 9 de octubre de 2025 entrará en vigor el **Artículo 5 quater** del Reglamento (UE) nº 260/2012, de 14 de marzo de 2012, por el que se establecen requisitos técnicos y empresariales para las transferencias y los adeudos domiciliados en euros, según la redacción dada por el Reglamento (UE) 2024/886 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de marzo de 2024.

El Reglamento (UE) 2024/886 señala que la seguridad de las transferencias en euros, tanto inmediatas como no inmediatas, es fundamental para aumentar la confianza de los usuarios de servicios de pago para enviar y recibir transferencias y garantizar su uso. Con arreglo a la Directiva (UE) 2015/2366, **el único factor determinante de la correcta ejecución de la operación con respecto al beneficiario es el identificador único (IBAN)**, definido en dicha Directiva, y **los proveedores de servicios de pago (las entidades financieras) no están obligados a verificar el nombre del beneficiario**. **Los proveedores de servicios de pago deben tener implantadas medidas sólidas y actualizadas de detección y prevención del fraude, diseñadas para evitar que se envíe una transferencia a un beneficiario no deseado como consecuencia de un fraude o error**, dado que el ordenante podría no poder recuperar los fondos antes de que se abonen en la cuenta del beneficiario.

Los proveedores de servicios de pago deben ofrecer un servicio de garantía de la verificación del beneficiario al que el ordenante tenga la intención de enviar una transferencia (**servicio de garantía de la verificación**). Para evitar fricciones o retrasos indebidos en el tratamiento de la operación, el proveedor de servicios de pago del ordenante debe prestar dicho servicio inmediatamente después de que este facilite la información pertinente sobre el beneficiario y antes de que se le ofrezca la posibilidad de autorizar la transferencia.

Algunos atributos del nombre del beneficiario a cuya cuenta el ordenante desea realizar una transferencia, como la presencia de signos diacríticos o diferentes transliteraciones posibles de nombres en otros alfabetos, diferencias entre los nombres de uso habitual y los nombres indicados en los documentos oficiales, podrían dar lugar a una situación en la que el nombre del beneficiario facilitado por el ordenante y el nombre asociado al identificador de la cuenta de pago que se especifica en el punto 1, letra a), del anexo del Reglamento (UE) n.o 260/2012 (identificador de la cuenta de pago), que fue facilitado por el ordenante, no coinciden de forma exacta, pero sí casi exacta. En tales casos, para evitar una fricción indebida en el tratamiento de las transferencias en euros y facilitar la decisión del ordenante sobre si proceder o no a la operación prevista, el proveedor de servicios de pago debe indicar al ordenante el nombre del beneficiario asociado al identificador de la cuenta de pago facilitado por el ordenante.

Autorizar una transferencia en la que no se haya verificado el beneficiario puede dar lugar a la transferencia de fondos a un beneficiario no intencionado. **Los proveedores de servicios de pago no deben ser considerados responsables de la ejecución de una operación enviada a un beneficiario no intencionado** por causa de un identificador único incorrecto, tal como se establece en el artículo 88 de la Directiva (UE) 2015/2366, en la medida en que los proveedores de servicios de pago **hayan prestado correctamente el servicio que garantice la verificación**. No obstante, **cuando los proveedores de servicios de pago no presten correctamente dicho servicio y esto dé lugar a una operación de pago ejecutada de manera defectuosa, dichos proveedores de servicios de pago deberán reembolsar sin demora el importe transferido al ordenante** y, cuando proceda, restablecer el saldo de la cuenta de pago en la cual se haya efectuado el adeudo a la situación en la que habría estado si no hubiera tenido lugar la operación de pago. Los proveedores de servicios de pago deben informar a los usuarios

de servicios de pago de las consecuencias que la decisión de estos últimos de desatender una notificación facilitada con arreglo al presente Reglamento modificativo tenga con respecto a la responsabilidad y los derechos al reembolso de los usuarios de los servicios de pago.

1.5 Controles sobre los datos maestros de terceros

Para combatir la ciberdelincuencia en el sistema de pagos, fundamentalmente son necesarias dos cosas:

a) Que exista un sistema de control interno bien establecido, **con procedimientos de gestión de la tesorería escritos debidamente aprobados y comunicados** que incluyan:

- la gestión de pagos,
- el mantenimiento del FMT, describiendo con detalle el procedimiento de alta y modificación de datos de terceros y de cuentas bancarias,
- las personas autorizadas para cada operación, por ejemplo, para realizar el alta y modificación del FMT y para aprobar los cambios,
- los cambios en el FMT (nuevos proveedores, cambios de datos bancarios, ...) se procesan solo después de que se hayan obtenido las aprobaciones adecuadas, de acuerdo con el principio de mínimo privilegio.
- una adecuada segregación de funciones,
- las altas y variaciones de datos **solo** se pueden hacer de forma electrónica a través de la sede electrónica (excepto para los no obligados legalmente),
- cualquier cambio en los datos del IBAN donde se realizan pagos debe estar justificado mediante un certificado de titularidad real o **preferentemente** mediante el servicio Iberpay integrado con el ERP,
- las declaraciones juradas de titularidad de cuenta corriente no se deben utilizar por los riesgos de falsedad documental,
- si el IBAN que aparece en la factura electrónica no coincide con el que consta en el FMT, no se pagará la factura a aquel IBAN sin verificarlo a través de Iberpay (hasta el 9/10/2025). Solo se pagará al que conste en el FMT, previa aclaración de la cuestión.
- En ocasiones los procedimientos de las entidades auditadas contemplan declaraciones responsables para acreditar la titularidad de las cuentas en el alta terceros y cuentas bancarias en el FMT. Este tipo de requisito o control, aunque es legal (art. 69 Ley 39/2015), no es un control tan robusto y fiable como los certificados o verificaciones con servicios *web* (tipo Iberpay) y representará un mayor riesgo.
- A partir del 9/10/2025 se actualizarán los procedimientos de comprobación del IBAN según se ha comentado en el apartado 1.4 anterior.

b) Establecer una **adecuada ciberseguridad** y controles generales de tecnologías de la información (CGTI) de acuerdo con el Esquema Nacional de Seguridad (ENS) que respalden los controles de procesamiento de la información, ya que de otra forma no serán fiables. Los controles sobre los FMT son especialmente dependientes de los CGTI y estos deben contemplar:

- la protección perimetral de la red,
- controles de acceso al ERP (módulo FMT) bien configurados. Se revisará que los CGTI *D.1 Uso controlado de privilegios de administración* y *D.2 Gestión de usuarios* funcionan eficazmente, bajo el principio de mínimo privilegio que establece el ENS.
- se mantiene un fichero histórico con todos los cambios en los datos maestros, incluyendo quién los realizó.

Los principales ***objetivos de control*** relativos a los datos maestros son los siguientes:

- Las altas y modificaciones deben ser realizadas por personas autorizadas, de forma exacta y completa.
- Las altas y modificaciones deben ser registradas y archivadas de forma que se mantenga la pista de auditoría (*logs*).

Anexo 1 B Consideraciones y ejemplos sobre los procedimientos de pago

1. Requisitos técnicos establecido en el Reglamento nº260/2012 del Parlamento Europeo y del Consejo de 14 de marzo de 2012 por el que se establecen requisitos técnicos y empresariales para las transferencias y los adeudos domiciliados en euros.

El artículo 5.1 establece que los proveedores de servicios de pago efectuarán transferencias y adeudos domiciliados con arreglo a los siguientes requisitos:

a) Deberán utilizar el identificador de cuenta de pago, el número IBAN.

b) Deberán utilizar los formatos de mensaje establecidos en la norma ISO 20022 XML.

El Reglamento señala que la «norma ISO 20022 XML» es la norma para la elaboración de mensajes financieros electrónicos, según lo definido por la ISO, relativa a la representación física de las operaciones de pago en sintaxis XML, de acuerdo con las disposiciones mercantiles y las directrices de aplicación de los regímenes de operaciones de pago comunes a toda la Unión comprendidas en el ámbito del presente Reglamento.

En resumen, las órdenes de pago emitidas por las entidades públicas a las entidades financieras o proveedores de servicios de pago (PSP) en la terminología del Reglamento debe emitirse con el formato de la norma ISO 20022 XML.

2. Normas del SEPA[10]

Qué significa SEPA

SEPA son las siglas en inglés de Single Euro Payments Area, es decir, Zona Única de Pagos en Euros. Se trata de una iniciativa por la que se establece una verdadera zona integrada de pagos europeos en euros en los que dichos pagos están sujetos a un conjunto uniforme de estándares, normas y condiciones.

La transferencia SEPA es un instrumento de pago básico para efectuar abonos en euros, sin límite de importe, entre cuentas bancarias de clientes en el ámbito de la SEPA, de forma totalmente electrónica y automatizada.

Mensajes ISO 20022 XML de iniciación de pagos

El gráfico siguiente muestra el ámbito que cubren los mensajes ISO 20022 para iniciación de pagos.

En la publicación "Órdenes en formato ISO 20022 para emisión de transferencias y cheques en euros" de la AEB se especifican los aspectos técnicos del mensaje de pagos que se debe enviar a las entidades financieras. En la práctica podemos encontrarnos con que la entidad denomina a estos documentos como ***Cuaderno 34-XML o ISO 20022 XML***. En esta guía usamos la primera.

El Cuaderno 34-XML para la presentación de transferencias, cheques, pagarés y pagos domiciliados, es el fichero de pagos en formato xml, con el que el cliente ordenante presenta las órdenes en formato estándar ISO 20022 XML para la emisión de transferencias en euros y en divisas, y cheques, pagarés y pagos domiciliados en euros.

[10] Fuente: Órdenes en formato ISO 20022 para emisión de transferencias y cheques en euros, noviembre 2023, AEB. (https://s2.aebanca.es/wp-content/uploads/2023/11/folleto.-rdenes-en-formato-iso-20022-para-emisin-de-transferencias-y-cheques-en-euros-noviembre-2023-v102.pdf).

El lenguaje XML (Extensible Mark-up Language) es un metalenguaje de etiquetas creado para el intercambio de información estructurada entre diferentes plataformas que permite definir un formato por medio de esquemas xsd, los cuales determinan qué elementos puede contener un documento XML, cómo están organizados, y qué atributos y de qué tipo son los que pueden tener dichos elementos. Mediante el uso del esquema pain.001.001.03.xsd se puede, además, verificar la validez de la forma y contenido de la información intercambiada.

3. Ejemplos de Gestión de los pagos a acreedores desde cuentas operativas (ni ACF ni PJ) en una entidad local.

El procedimiento de gestión de pagos a acreedores de la entidad parte de los documentos contables que acreditan un saldo a pagar al acreedor derivado de la tramitación de gastos, presupuestarios o no presupuestarios.

Cuando se va a realizar un pago, de acuerdo con el plan de tesorería aprobado, la Tesorería municipal inicia el proceso en la aplicación CONTABLE/TESORERÍA seleccionando los acreedores cuya ordenación de pagos se va a realizar. La prioridad de los acreedores a incluir en la simulación se establece en el plan de tesorería aprobado.

Los pagos se hacen normalmente mediante transferencia bancaria y pueden ser de varios tipos según su circuito de tramitación, los más habituales son:

- Tipo A. Transferencias masivas. Se cursa una orden de pago a la entidad financiera por un importe global que se genera en la aplicación CONTABLE/TESORERÍA. El detalle individualizado de los pagos a realizar se incluye en un fichero con formato estándar bancario (Cuaderno 34-XML) que se envía a la entidad financiera mediante un circuito seguro de transmisión de ficheros.
- Tipo B. Transferencias masivas específicas: pago de nóminas, retenciones judiciales y pensiones alimenticias. Generalmente se realizan una vez al mes. El procedimiento de tramitación es el mismo que en el tipo A.
- Tipo C. Transferencia manual con documento cobratorio. En este caso el oficio de orden de pago al banco se elabora en la aplicación CONTABLE/TESORERÍA, pero va acompañado de un documento cobratorio. Requiere la apertura de un expediente para la obtención del documento (pagos de IVA, IRPF, SS, pago a juzgados, …).

Canales de transmisión de los ficheros entre el ayuntamiento y la entidad financiera. Los ayuntamientos podrán enviar sus ficheros (Cuaderno 34-XML) a través de los siguientes canales:

- Transmisión a través de la página web de la entidad financiera.
- Transmisión Host to Host (protocolos Editran, XCom, Swiftnet). Estos protocolos de transmisión son utilizados principalmente por entidades con un gran volumen de pagos.
- Transmisión desde la oficina gestora. El ayuntamiento deberá entregar el fichero mediante el soporte convenido con la oficina gestora, usualmente un pendrive USB conteniendo el fichero a procesar. Este procedimiento **NO** es recomendable.

Procedimiento ordinario: Transmisión Host to Host

Los documentos generados en la aplicación CONTABLE/TESORERÍA se envían al portafirmas del gestor de expedientes de la entidad de manera automática y siguen las fases que se detallan a continuación.

a) Tramitación del proceso de firma del documento de orden de pago al banco y del documento de oficio de propuesta de ordenación en el portafirmas.

   Los firmantes van recibiendo, por el orden establecido en el portafirmas en el flujo del procedimiento, una notificación para revisar los documentos y firmar electrónicamente para aprobar o rechazar el pago. Además de las tres personas que deben de firmar la orden de pago, también revisa y firma los pagos a realizar el jefe del servicio de Tesorería. En este punto, los firmantes pueden revisar uno a uno los documentos que se van a firmar y los perceptores y cuentas bancarias a las que se va a realizar el pago.

   Una vez se ha aprobado el pago por todos los firmantes, ya estarán disponibles los documentos firmados para su envío.

   La disposición de fondos de las cuentas operativas del Ayuntamiento es mancomunada y requiere siempre la firma de tres de los autorizados para la disposición de fondos: Tesorero, Interventor y Concejal, o sus sustitutos.

La fiscalización formal y material del pago prevista en la normativa aplicable a las Entidades Locales se realiza en esta fase de la tramitación.

b) Contabilización de la relación de los pagos ordenados

En este punto se genera el documento contable de pago presupuestario o no presupuestario, y el fichero en formato bancario Cuaderno 34-XML a remitir a la entidad financiera.

Los apuntes contables de pago se realizan en una cuenta contable de tesorería "transitoria" hasta que se "concilien" con los movimientos reales en banco enviados por la entidad financiera al día siguiente (cuaderno 43), momento en que contabilizan en la cuenta contable de tesorería definitiva.

Este fichero (Cuaderno 34-XML) se almacena en una carpeta del sistema CONTABLE/TESORERÍA a la que **sólo** tiene acceso el propio sistema CONTABLE/TESORERÍA para procesos automatizados o los administradores del sistema.

c) Envío de ficheros al banco

El responsable de pagos remite mediante correo electrónico (con los protocolos SPF, DKIM y DMARC[11]) la orden de pago firmada electrónicamente a la entidad financiera seleccionada que va a realizar el pago.

Adicionalmente, y de forma **automatizada** se envía mediante el sistema EDITRAN el fichero de pagos Cuaderno 34-XML a la entidad financiera. Este envío se realiza a través de la aplicación CONTABLE/TESORERÍA, mediante una interfaz automatizada entre ambos sistemas. **No** se admite su envío por email o fax, ya que no cumple los requisitos de la PSD2.

d) Recepción de la orden de pago y del fichero de pagos por la entidad financiera

La entidad financiera recibe la orden de pago por correo electrónico y debe verificar que está firmada electrónica y mancomunadamente por las tres personas con autorización para disponer fondos.

También verifica que el importe de la orden de pago coincide con el importe total del fichero de pagos enviado a través de EDITRAN.

Procedimiento extraordinario: Transmisión a través de la página web de la entidad financiera

El procedimiento es similar al anterior, pero el fichero de pagos generado (Cuaderno 34-XML) se almacena en una carpeta del sistema a la que tienen acceso N personas (las N personas autorizadas deben ser las mínimas necesarias), incluyendo el personal de tesorería. El fichero Cuaderno 34-XML se carga manualmente en la página web de la entidad financiera. El resto del procedimiento es similar al anterior.

El riesgo principal aquí es la protección de la integridad del Cuaderno 34-XML frente a accesos no autorizados a la carpeta en la que se guarda.

[11] El Centro Criptológico Nacional publicó en mayo de 2024 el informe de buenas prácticas **"BP/33: Recomendaciones de Seguridad en el correo electrónico, DMARC"**. En este documento se explica el concepto de DMARC (*Domain-based Message Authentification Reporting and Conformance*), que es un protocolo de validación de correo electrónico diseñado para proteger los dominios de correo electrónico de la suplantación de identidad, la integridad de la información y otras formas de abuso en el correo electrónico, como el fraude y el phishing.

Se examinan las repercusiones que se desencadenan al aplicar DMARC, detallando cómo esta medida puede influir en la identificación y prevención de intentos de suplantación de identidad (phishing) y otros ciberataques relacionados con el correo electrónico. Se presentan ejemplos concretos de situaciones que pueden surgir al implementar DMARC y se proporciona información esencial para comprender cómo esta herramienta contribuye a garantizar la integridad y autenticidad de los mensajes electrónicos.

Antes de DMARC, ya existían SPF (*Sender Policy Framework*) y DKIM (*DomainKeys Identified Mail*), que son métodos para verificar si los correos electrónicos provienen de fuentes legítimas. Sin embargo, estos métodos tenían limitaciones, especialmente en cómo se trataban los mensajes que fallaban en estas verificaciones. DMARC utiliza las tecnologías de SPF y DKIM antes mencionadas para verificar que los mensajes de correo electrónico procedentes de un dominio sean auténticos y no hayan sido alterados en tránsito.

Programa de auditoría:

Al diseñar los programas se seleccionarán aquellas pruebas que respondan mejor a los riesgos significativos identificados 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 y de cada tipo de entidad.
Cada OCEX podrá sustituir este programa por los que tenga establecidos como estándar.

Hoja sumaria

Trabajo a realizar:

1. Preparar una hoja sumaria del área y obtener los saldos individuales a 31 de diciembre, de las distintas cuentas comprobando que coinciden con la contabilidad.

   Será la información que debe figurar en la nota __ del modelo de la memoria. Cruzar el total con el epígrafe correspondiente del balance (subgrupo 57).

   Mostrar también los movimientos de cobros y pagos de todas las cuentas para visualizar el volumen de actividad de cada cuenta.

2. Cajas.

   Cruzar las existencias de fondos líquidos de cada caja con las actas de arqueo que deben venir unidas a las cuentas anuales de la entidad.

3. Cuentas bancarias.

   Cruzar los saldos a favor de la entidad en cada cuenta de entidades bancarias con las notas o certificaciones que deben venir unidas a las cuentas anuales de la entidad.

   En caso de haberse solicitado a la entidad un certificado de cuentas bancarias, cruzar los datos con el certificado obtenido.

   Cuando no coincida saldo contable y bancario cruzar saldos con la correspondiente conciliación bancaria.

4. Solicitar una comunicación comprensiva de todas las cuentas bancarias de la entidad con las que han operado durante el ejercicio y solicitar los contratos firmados vigentes con las entidades financieras y analizar entre otros aspectos, los siguientes para cada cuenta bancaria:

   - ✓ Entidad bancaria.
   - ✓ Número de cuenta y tipo.
   - ✓ Título de la cuenta.
   - ✓ Naturaleza de la cuenta (si se trata de una cuenta de provisión de fondos, restringida de recaudación, restringida de pagos, etc.).
   - ✓ Autorización para la apertura.
   - ✓ Fecha de apertura, de última prórroga y, en su caso, de cancelación.
   - ✓ Describir el tipo de restricciones de la cuenta.
   - ✓ Tipo de interés aplicable a saldos deudores y acreedores, periodicidad con la que se liquidan y plazos de ingreso.
   - ✓ Régimen de firmas y personas autorizadas para disponer de los fondos, así como la comunicación a la entidad bancaria de las posibles modificaciones existentes. Indicar en su caso, la situación en que una firma autorizada se ha mantenido con posterioridad a que el titular dejase de desempeñar el cargo que determinó dicha autorización de firma.
   - ✓ Obtener el importe total de cobros y pagos gestionados a través de cada cuenta bancaria.

Información complementaria:

Art. 194 a 199 del TR LRHL

Art 5 del Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional

Conocer y comprender los procedimientos de gestión de tesorería y el control interno

Trabajo a realizar:

5. Solicitar si existen procedimientos de gestión de tesorería y revisarlos.
   Solicitar las bases de ejecución del presupuesto.
6. Completar el cuestionario "*Anexo 1 Documentación del conocimiento del proceso de gestión de tesorería"* de la GPF-OCEX 1957.

   Considerar al menos los siguientes aspectos:

   a. Estructura organizativa del departamento de Tesorería.
   b. La forma habitual de ingresos y pagos.
   c. La segregación de funciones.
   d. El puesto de tesorero.
   e. Identificar las aplicaciones informáticas utilizadas en la contabilización y gestión de la tesorería. Señalar quiénes tienen acceso a las aplicaciones de gestión de tesorería o a las opciones de tesorería de la aplicación de contabilidad.
   f. Obtener información sobre el procedimiento para dar de alta terceros y sus cuentas bancarias en las aplicaciones y quienes son los encargados de tramitarlos y aprobarlos (no duplicar si ya se ha hecho el trabajo en otras áreas).
   g. Averiguar si es posible cambiar el tercero y/o cuenta bancaria en un documento de obligación reconocida ya contabilizado. Si es posible, averiguar quién puede hacerlo (no duplicar si ya se ha hecho el trabajo en otras áreas).
   h. Obtener información sobre la carpeta en la que se depositan los ficheros bancarios de pagos y si está restringido el acceso a las personas que lo necesitan exclusivamente.
   i. Comprobar que la Tesorería sirve al principio de unidad de caja, mediante la centralización de todos los fondos y valores generados por operaciones presupuestarias y extrapresupuestarias.
   j. Comprobar si las existencias de efectivo en caja están reglamentariamente limitadas y, en este caso, si se ajustan a dichas limitaciones.
   k. Realizar un flujograma general del procedimiento, y de los subprocesos más relevantes.
7. Analizar conflictos de segregación de funciones.
8. 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.
9. En las entidades más grandes, considerar la conveniencia de solicitar la ayuda de los expertos en auditoría de sistemas de información.
10. 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.
11. Revisar la valoración del riesgo para esta área.
12. Identificar los CPI relevantes relacionados con el proceso de gestión y los CGTI que los soportan.
13. Identificar y revisar, en su caso, las interfaces de la aplicación con la que se gestiona la tesorería con otras relevantes (contabilidad si no es la misma, ingresos, generación y envío de ficheros a las entidades financieras, …).
14. Se debe realizar o discutir este análisis en una reunión del equipo (ver GPF-OCEX 1513).
15. Documentar el trabajo según el Anexo 1 de la GPF-OCEX 1957.
16. Concluir y señalar la valoración del riesgo para esta área.

    Hacer un resumen de las incidencias detectadas y proponer las sugerencias y recomendaciones que se consideren oportunas para mejorar el control interno y comentarlas con la dirección de la entidad.

Información complementaria:

Revisar los controles generales de TI

***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 tesorería se deberá recabar la colaboración del auditor de sistemas.

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

17. Solicitar la colaboración de expertos en auditoría de sistemas.
18. 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.
19. Realizar las pruebas de eficacia del diseño y de eficacia operativa (pruebas de controles).
20. Concluir sobre la situación de los CGTI, su impacto en los CPI y si tiene efecto en la opinión de auditoría.

Información complementaria:

Plan de disposición de fondos/de tesorería

Trabajo a realizar:

21. Comprobar que la entidad ha elaborado el Plan de disposición de fondos exigido por la normativa y revisar el control realizado por el interventor y si existen reparos.

Información complementaria:

El artículo 187 del Texto Refundido de la Ley Reguladora de las Haciendas Locales (TRLRHL), establece: «La expedición de las órdenes de pago habrá de acomodarse al **plan de disposición de fondos** de la tesorería que se establezca por el presidente que, en todo caso, deberá recoger la prioridad de los gastos de personal y de las obligaciones contraídas en ejercicios anteriores». El Plan de Disposición de Fondos es un instrumento necesario para la gestión de la tesorería; y constituye la herramienta para regular la liquidez del sistema financiero local.

El interventor en virtud del artículo 214 del TRLRHL, debe fiscalizarlo formulando reparo en su caso.

Por otra parte, la DA 4ª de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera indica: «Las Administraciones Públicas deberán disponer de **planes de tesorería** que pongan de manifiesto su capacidad para atender el pago de los vencimientos de deudas financieras con especial previsión de los pagos de intereses y capital de la deuda pública». En vigor durante 2012.

Si bien en vigor a partir del 1 de enero de 2013, el contenido mínimo del **Plan de Tesorería** aparece recogido en el apartado 8 art. 16 de la Orden HAP/2105/2012, de 1 de octubre (BOE del 5), por el que se desarrollan las obligaciones de suministro de información previstas en la Ley Orgánica de Estabilidad Presupuestaria y Sostenibilidad Financiera, que establece que, antes del último día del mes siguiente a cada trimestre se deberán presentar «las actualizaciones de su Plan de tesorería y detalle de las operaciones de deuda viva». Esta remisión al Ministerio de Hacienda y Administraciones Públicas la debe hacer el Interventor del Ayuntamiento:

"8. Las actualizaciones de su Plan de tesorería y detalle de las operaciones de deuda viva que contendrá al menos información relativa a:

a) Calendario y presupuesto de Tesorería que contenga sus cobros y pagos mensuales por rúbricas incluyendo la previsión de su mínimo mensual de tesorería.
b) Previsión mensual de ingresos.
c) Saldo de deuda viva.
d) Impacto de las medidas de ahorro y medidas de ingresos previstas y calendario previsto de impacto en presupuesto.
e) Vencimientos mensuales de deuda a corto y largo plazo.
f) Calendario y cuantías de necesidades de endeudamiento.
g) Evolución del saldo de las obligaciones reconocidas pendientes de pago tanto del ejercicio corriente como de los años anteriores.
h) Perfil de vencimientos de la deuda de los próximos diez años.

Cajas (570-574)

Trabajo a realizar:

22. Obtener una relación de Cajas existentes en la Entidad y sus responsables y comprobar:
    a. Que las actas de arqueo unidas a la cuenta general están adecuadamente cumplimentadas y formalizadas. *(Firmadas por el ordenador de pagos (Alcalde), por el responsable administrativo de la gestión financiera (Tesorero) y por el órgano de control interno (Interventor)).*
    b. que las existencias reales con los datos contables a dicha fecha. Investigar las posibles diferencias.
    c. que la existencia en efectivo más la documentación justificativa de pagos realizados que se encuentren pendientes de registrar en el momento de efectuar el arqueo no superan las cuantías máximas de existencias en efectivo autorizadas

23. Realizar un **arqueo sorpresivo** sobre las existencias en las diferentes cajas de la entidad.

    El recuento de los fondos y demás justificantes deberá realizarlo el Cajero pagador en presencia del funcionario de la Intervención o del Tesorero.

    Detallar los resultados de los arqueos en documentos firmados tanto por personal del equipo como de los responsables de la entidad (tesorero) que deben estar presentes durante el arqueo.

24. Revisar los movimientos de efectivo para detectar y analizar partidas poco usuales o extraordinarias.

25. Concluir sobre la razonabilidad de los saldos de caja.

Información complementaria:

Los riesgos más destacados que se pretenden analizar en este apartado son:

Riesgos de incumplimiento:

- Existencia de cajas indebidamente constituidas incumpliendo la normativa aplicable.
- Inadecuada utilización de los fondos.

Riesgos de ineficacia e ineficiencia:

- Inexistencia de una relación completa de Cajas pagadoras, Subcajas, Habilitaciones y unidades administrativas adscritas al organismo/entidad que gestionen fondos de tesorería, así como la falta de información sobre los pagos gestionados por cada una de ellas, impidiendo llevar el control sobre las cajas y el seguimiento de su actividad.
- Ausencia de controles de caja a través de conciliaciones periódicas, circularizaciones periódicas, etc.
- Ausencia de restricciones en el uso de dinero efectivo mediante segregación de funciones, firmas mancomunadas, etc.

El trabajo realizado debe permitir concluir sobre:

- La adecuación normativa de las cajas pagadoras, subcajas, habilitaciones, etc. que gestionan el efectivo existente en el Organismo/Entidad. El cumplimiento de la normativa vigente en cuanto a nombramiento de Cajeros, creación, mantenimiento de existencias en efectivo, etc.
- El cumplimiento de la normativa vigente respecto al control de las cajas de efectivo mediante la realización de arqueos (la no superación de las cuantías máximas de efectivo autorizadas, las posibles diferencias con los registros en libros, etc.).

Cuentas en entidades bancarias (571-573-575-577)

Trabajo a realizar:

26. Comprobar que todas las cuentas han sido aperturadas cumpliendo la normativa aplicable.

    Analizar la relación de cuentas bancarias proporcionada por el auditado.

    Sin perjuicio de otros aspectos que el auditor considere relevantes, verificar que las cuentas bancarias cumplen con los requerimientos legales para su creación, mantenimiento y, en su caso, extinción.

Circularización

27. Solicitar a la entidad la preparación de las cartas de confirmación de saldos bancarios. (*la información a solicitar a los bancos dependerá del alcance de la fiscalización, por lo que los anexos a remitir deberán ser adaptados*).

    La entidad debe preparar las cartas de circularización, conforme a los modelos facilitados al efecto por el auditor, de <u>todas</u> las entidades bancarias en las que hay o haya habido alguna cuenta bancaria durante el ejercicio auditado.

Una vez firmada por la entidad, el auditor las envía.

La carta debe decir claramente que la respuesta ha de enviarse directamente al auditor.

Se pretende que:

i. El banco conteste detallando todas y cada una de las cuentas que la entidad tiene o ha tenido abiertas en el período auditado, especificando su saldo a 31 de diciembre del ejercicio auditado, haciendo constar en su caso si hay alguna restricción al uso de alguno.

ii. Que el banco informe sobre posibles pasivos (muy importante) si hay préstamos o anticipos.

iii. Total, de las letras: descontadas y pendientes de cobro, enviadas en gestión de cobro y pendientes impagadas en poder del banco.

iv. Pormenores sobre toda clase de valores a favor de la entidad auditada que hayan estado en poder del banco, en custodia o en depósito.

v. Cualquier otra información relativa a la entidad auditada con el banco.

vi. Personas que figuran con autorización en el banco para la firma de cheques, letras, endosos, etc., indicando cuántas de ellas son indispensables y combinaciones de las mismas.

28. Añadir el papel de trabajo de control de circularización, actualizándolo convenientemente.

Realizar las siguientes comprobaciones:

- ✓ Número de las cuentas.
- ✓ Naturaleza de las cuentas.
- ✓ Tipo de interés.
- ✓ Firmas autorizadas.
- ✓ Que el saldo, según la información obtenida mediante la circularización coincide con el reflejado en el correspondiente registro contable.
- ✓ Deudas existentes.
- ✓ El número de tarjetas de crédito o débito disponibles.

Analizar los datos proporcionados por las entidades financieras**:** Sin perjuicio de otros aspectos que el auditor considere relevantes, analizar la fiabilidad e integridad de los datos proporcionados por el ente auditado, una vez analizados los registros de las entidades financieras. Si los datos proporcionados fueran poco fiables, incompletos, incorrectos o no íntegros, explicar las razones.

29. En los casos de no respuesta a la primera petición tras un periodo determinado (dos semanas, por ejemplo), remitir la segunda petición.

30. En los casos de no respuesta a la segunda petición, solicitar al personal responsable de la entidad local que se ponga en contacto con la entidad bancaria para que nos conteste de forma inmediata.

31. Revisar las respuestas de las entidades bancarias.

Cruzar los saldos confirmados por los bancos con las conciliaciones bancarias (que deben estar unidas a la cuenta general) en los supuestos que no coincidan con los saldos contables, o con la hoja sumaria de tesorería en los supuestos de coincidencia.

Verificar que las firmas confirmadas y la forma de disposición de los fondos son correctas.

Cruzar toda la información confirmada por los bancos con la información contable de la entidad, para las áreas objeto del alcance de la fiscalización.

Conciliaciones bancarias

32. Verificar que las conciliaciones bancarias, a la fecha de cierre contable, están adecuadamente realizadas y revisadas. Comprobar:

- La exactitud matemática de las conciliaciones.
- Cotejar saldos con extractos bancarios/contestaciones y con contabilidad.
- Analizar con documentación soporte las partidas en conciliación que sean significativas o sospechosas.
- Concluir sobre la razonabilidad de cada una de las conciliaciones.
- Comentar el resultado de la prueba y proponer los ajustes, reclasificaciones o recomendaciones que resulten oportunos.

Otros

33. Verificar si existen cuentas restringidas de ingresos o de gastos, y en caso afirmativo comprobar que sus saldos al cierre están incluidos en el balance.
34. **Analizar los cobros, pagos y saldos de las operaciones con mayores riesgos**: Sin perjuicio de otros aspectos que el auditor considere relevantes, verificar aquellas operaciones como posibles descubiertos en cuentas, la adecuada justificación de las operaciones en el exterior, las realizadas por un agente mediador o equivalente, etc.
35. **Analizar las operaciones extrapresupuestarias**: Sin perjuicio de otros aspectos que el auditor considere relevantes, verificar las operaciones extrapresupuestarias, con objeto de detectar entradas y salidas de fondos no justificadas, verificar la existencia de operaciones anómalas por la atipicidad del importe, la existencia de salidas/entradas de mismo importe, etc.
36. En el caso de **cuentas sin movimientos** durante el periodo auditado, analizar el saldo el último día del período auditado, los días sin movimiento, las causas de su mantenimiento, así como los posibles gastos y rentabilidades asociados a las mismas.
37. **Analizar los movimientos de una muestra de cuentas**: Sin perjuicio de otros aspectos que el auditor considere relevantes, analizar la situación de las cuentas sin movimientos, los motivos de esa falta de movimientos, así como los posibles gastos generados por las mismas.
38. **Corte de operaciones**: consiste en obtener los extractos bancarios de unos días anteriores y posteriores a la fecha de referencia (Cierre) y verificar el movimiento habido en los saldos de la cuenta y su correcta imputación al período correspondiente.
39. Concluir.

Información complementaria:

Los riesgos más destacados que se pretenden analizar en este apartado son:

Riesgos de incumplimiento:

- Incumplimiento de los requisitos legales de apertura, mantenimiento o cierre de las cuentas bancarias.
- Incumplimientos legales en la gestión del pago de los expedientes de gasto, de las nóminas y de los fondos en el exterior.
- Uso inadecuado de los fondos existentes por falta de mecanismos de control.

Riesgos de ineficacia e ineficiencia:

- Inexistencia de una relación íntegra de todas las cuentas bancarias abiertas por la entidad, lo que puede impedir el adecuado control por parte del organismo/entidad de las cuentas bancarias y su estado.
- Inexistencia de registros actualizados sobre la totalidad de cobros y pagos realizados, lo que puede derivar en un inadecuado uso de los fondos.

El trabajo realizado debe permitir concluir sobre:

- El cumplimiento de los requerimientos legales para la creación, mantenimiento y, en su caso, extinción de las cuentas bancarias abiertas por la entidad.
- El volumen de actividad de la Caja pagadora a través de los saldos totales de cobros y pagos.
- El grado de integridad y fiabilidad de la información proporcionada por el gestor, con respecto a la información suministrada por las entidades financieras a través de las circularizaciones realizadas.
- El cumplimiento de la normativa aplicable con respecto a la rentabilidad y/o costes generados por las cuentas corrientes abiertas en las entidades financieras.
- Si los cobros y pagos registrados en las cuentas bancarias están adecuadamente justificados y contabilizados.

Revisión de las conciliaciones bancarias que ha realizado la entidad:

La conciliación consiste en cuadrar, a la fecha del cierre, el saldo según los libros de contabilidad de la entidad con el saldo del extracto o confirmación directa del banco. Además de verificar la exactitud aritmética de la conciliación, desde el punto de vista de la auditoría, hay que analizar con detenimiento las partidas de la misma, verificando su naturaleza, antigüedad e importe. Una partida que aparezca constantemente (años) en la conciliación puede ser indicio de alguna irregularidad.

Otras cuentas de tesorería

Trabajo a realizar:

40. 578 Movimientos internos de tesorería. (Utilización opcional). Verificar que presenta saldo cero al cierre del ejercicio. Revisar si han tenido lugar operaciones significativas durante el ejercicio y comprobar para una muestra su adecuado tratamiento contable.
41. 579. Formalización. Ídem que el punto anterior.
42. 554 y 555 Cobros y pagos pendientes de aplicación. Analizar el saldo al cierre y movimientos del año si son significativos. Comprobar para una muestra significativa si su utilización es la adecuada.
43. Concluir.

Información complementaria:

Pagos a justificar (558)

Trabajo a realizar:

44. *Comprobar si las **bases de ejecución** contienen las normas reguladoras de la expedición de órdenes de pago a justificar y que éstas han sido informadas por el interventor, conforme a lo establecido en el artículo 190.2 del* TRLRHL y en el artículo 72.2 del RD 500/1990. También podrá incluirse la regulación de este procedimiento especial de pagos en los reglamentos o normas generales de ejecución presupuestaria de la Entidad.
45. Obtener del sistema de información contable, las órdenes de pago a justificar contabilizadas al debe de la cuenta 558.5 "Libramientos *para provisiones de fondos" y **seleccionar una muestra** representativa de los mismos que incluya pagos efectuados y pendientes de justificación, pagos efectuados, justificados y contabilizados y pagos pendientes de efectuar, a 31 de diciembre del ejercicio fiscalizado.*
46. *Verificar la adecuada **contabilización** de los libramientos seleccionados, conforme a lo dispuesto en la regla 33 de la ICAL. En caso de que la Entidad aplique el modelo básico, comprobar que los registros extracontables* permiten un adecuado seguimiento y control.
47. Veri*ficar la **adecuación a la legalidad** de la muestra de pagos seleccionada, mediante la verificación de los siguientes aspectos, previstos en los artículos 69 a 71 del RD 500/1990 y a lo dispuesto en la normativa interna del ayuntamiento:*
    a) *Existe una propuesta motivada formulada por el responsable del gasto.*
    b) *La orden de pago a justificar ha sido aprobada por el órgano competente para autorizar el gasto.*
    c) *La expedición de la orden a justificar se acomoda al plan de disposición de fondos de la tesorería, establecido por el alcalde.*
    d) *El plazo máximo de tres meses para su justificación.*
    e) *El reintegro de los importes librados y no pagados o no justificados en el plazo legal.*
    f) *No se han expedido nuevas órdenes de pagos a justificar a perceptores que no hubieran justificado órdenes anteriores por los mismos conceptos.*
    g) *Que los pagos efectuados se han aplicado a la finalidad autorizada.*
    h) *Que los justificantes reúnen los requisitos formales previstos reglamentariamente.*
    i) *Aquellos otros extremos contemplados en la normativa del ayuntamiento.*
48. *Concluir.*

Información complementaria:

Se debe efectuar la imputación presupuestaria en el momento de la expedición y pago de la orden librada a justificar, lo que origina un cargo y un abono en la cuenta 5585. Conforme se van efectuando los pagos al acreedor último se carga la cuenta 5580, la cual se abona a la justificación de los gastos. Si el reintegro del sobrante tiene lugar en un ejercicio posterior debe contabilizarse como un ingreso presupuestario, si es en el mismo ejercicio será un menor gasto presupuestario. A 31 de diciembre todos los gastos realizados por el perceptor, pendientes de justificación, se abonarán a la cuenta 5586. En las entidades que apliquen la Instrucción del modelo básico no se realizan los cargos y abonos detallados en las cuentas de contabilidad financiera.

Anticipos de caja fija (558)

Trabajo a realizar:

49. Comprobar que las bases de ejecución contienen las normas reguladoras de los anticipos de caja fija y que éstas han sido informadas por el interventor, conforme a lo establecido en el artículo 75 del RD 500/1990. También podrá incluirse la regulación de este procedimiento especial de pagos en reglamentos o normas generales de ejecución presupuestaria aprobados por el Pleno.
50. Comprobar que las provisiones de fondos en concepto de caja fija se atienen a lo establecido en los artículos 73 y siguientes del RD 500/90, así como su adecuada contabilización, conforme a la regla 36 de la ICAL.
51. Obtener del sistema de información contable, los pagos efectuados a los acreedores finales con abono a las cuentas restringidas de tesorería de caja fija y cargo a la cuenta 558.1 "Provisiones de fondos para anticipos de caja fija pendientes de justificación" y seleccionar una muestra.
52. Verificar la adecuación a la legalidad de la muestra de pagos seleccionada, conforme a lo establecido en los artículos 73 y siguientes del RD 500/1990 y a lo dispuesto en la normativa interna del ayuntamiento, y su adecuada contabilización (regla 36 ICAL).
53. Operaciones pendientes de aplicar a presupuesto a 31 de diciembre. Comprobar su contabilización en la cuenta 413.
54. Concluir.

Información complementaria:

Los riesgos más habituales en este apartado son:

Riesgos de incumplimiento:

- Incumplimientos legales en la expedición de órdenes de PJ y de ACF (inexistencia de Acuerdo/ Resolución, superación de cantidades máximas, gastos imputables a conceptos presupuestarios no autorizados, etc.).

Riesgos de ineficacia e ineficiencia:

- Falta de calidad de las cuentas justificativas, pudiendo originar una inadecuada utilización de los fondos.
- Utilización abusiva del sistema de anticipos de caja fija, pagos a justificar o procedimientos equivalentes, con respecto al procedimiento ordinario de pago (pagos en firme).
- Procedimientos especiales de pago equivalentes diseñados que establezcan procedimientos ineficientes o desactualizados.
- Existencia de errores o incongruencias en la información contenida en los EST debidos a una mala gestión de la información y documentación que los soporta.

El trabajo realizado debe permitir concluir sobre:

- El cumplimiento de la normativa vigente en los procedimientos especiales de pago (normas que los establezcan, naturaleza de los gastos, órgano competente, tipos de pagos, etc.).
- Idoneidad y eficiencia de la gestión de los procedimientos especiales de pago (saldos de cajas de efectivo y/o cuentas, reintegros, pagos sin justificación, cuentas justificativas fuera de plazo, cuentas justificativas favorables, cuentas sin defectos, incidencias en el pago etc.).
- El cumplimiento de las obligaciones contables (llevanza de los libros y registros contables, cuentas justificativas y documentación que las acompaña, etc.).

9. Estado de Flujos de Efectivo.

Trabajo a realizar:

55. Verificar que las agrupaciones del EFE se estructuran como se indica a continuación:

    i. Flujos de efectivo de las actividades de gestión: son los que constituyen su principal fuente de generación de efectivo y, fundamentalmente los ocasionados por las transacciones que intervienen en la determinación del resultado de gestión ordinaria de la entidad. Se incluyen también los que no deban clasificarse en ninguna de las dos categorías siguientes, de inversión o de financiación.

    ii. Flujos de efectivo de las actividades de inversión: son los pagos que tienen su origen en la adquisición de elementos del inmovilizado no financiero y de inversiones financieras, tanto de corto como de largo plazo, no consideradas activos líquidos equivalentes a efectivo, así como los cobros procedentes de su enajenación o de

su amortización al vencimiento. Forman parte de estos flujos los cobros derivados de la venta de activos en estado de venta.

iii. Flujos de efectivo de las actividades de financiación: comprenden los cobros procedentes de la adquisición por terceros de títulos valores emitidos por la entidad o de recursos concedidos por entidades financieras o terceros, en forma de préstamos u otros instrumentos de financiación y, los correspondientes a aportaciones al patrimonio de la entidad o entidades propietarias. También comprenden los pagos realizados por amortización o devolución de los anteriores instrumentos de financiación y por reparto de resultados a la entidad o entidades propietarias.

iv. Flujos de efectivo pendientes de clasificación: recogen los cobros y pagos cuyo origen se desconoce en el momento de elaborar el estado de flujos de efectivo.

v. Efecto de las variaciones de los tipos de cambio: recoge, con el fin de permitir la conciliación entre las existencias de efectivo al principio y al final del período, el efecto de la variación de los tipos de cambio, sobre el efectivo y otros activos líquidos equivalentes que figuraran denominados en moneda extranjera. El valor en euros de estos últimos será el que corresponda al tipo de cambio de 31 de diciembre.

56. Verificar que en la elaboración del EFE la entidad pública ha tenido en cuenta las disposiciones previstas en el apartado 1 sobre "Normas de elaboración de las cuentas anuales" de la tercera parte del PGCP.

57. Verificar que el saldo de "efectivo y activos líquidos equivalentes al efectivo al final del ejercicio" del estado de flujos de efectivo coincide con los importes reflejados en el epígrafe de "Tesorería" del Balance de Situación.

Información complementaria:

Información de la memoria

58. Verificar la concordancia de la información en Memoria con la ofrecida por los registros contables, así como, si la memoria muestra la información exigida en el PGCP.

59. Verificar que el Estado del remanente de tesorería, incluido en el punto 24.6 de la memoria, se ha elaborado a partir de los saldos de las cuentas del PGCP a que se hace referencia en el cuadro del citado punto.

El remanente de tesorería total se obtendrá por la suma de los fondos líquidos más los derechos pendientes de cobro deduciendo las obligaciones pendientes de pago y agregando las partidas pendientes de aplicación de conformidad con los criterios que se establecen en la memoria.

Información complementaria:

Conclusión del área

60. Concluir sobre si se han alcanzado razonablemente los objetivos del área.

61. Redactar un resumen de los aspectos más importantes del área de tesorería, el trabajo realizado y las incidencias observadas.

62. Comentar las incidencias con los responsables y anotar sus comentarios y nuestra consideración.

63. Referenciar el análisis de las incidencias a las fichas correspondientes de AS1. Indicar para cada incidencia si es de carácter financiero o de legalidad, así como su consideración de salvedad, o a comentar solo en el interior del informe o recomendación de control interno a comentar en el interior del informe y en su caso en el apartado de recomendaciones.

64. Redactar la parte del proyecto de informe del área con el formato aplicable.

Información complementaria:

Al finalizar la fiscalización de esta área se deberá concluir sobre si, tras el trabajo realizado y el análisis de las evidencias obtenidas, se considera que se han alcanzado razonablemente los objetivos de auditoría y no se ha detectado ninguna incorrección de carácter significativo. En caso contrario se describirán las incorrecciones detectadas.