1. Introducción y objetivos de la guía

Las Normas Técnicas de Auditoría (ver MFSC-1310) tienen implícito un concepto fundamental: el auditor, al planificar una auditoría, debe realizar un análisis de los riesgos de auditoría que pueden existir al ejecutar el trabajo y emitir su informe; teniendo en cuenta ese análisis se 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, en síntesis, es el denominado enfoque de auditoría basado en el análisis de los riesgos (o enfoque de riesgo).

Muy esquemáticamente, las etapas de una auditoría ejecutada con el enfoque basado en el análisis de los riesgos son:

- Conocimiento de la entidad
- Análisis de las cuentas anuales auditadas: Identificación de los saldos, transacciones y clases de transacciones significativas. Identificación de las actividades, de los procesos de gestión significativos, de las aplicaciones que los soportan y de los flujos de datos relacionados.
- Valoración de los riesgos tanto a nivel global como de las afirmaciones e identificación de las áreas significativas.
- Revisión de los controles generales.
- Adquisición de un conocimiento de los procesos de gestión significativos, de las aplicaciones significativas y de las principales interfaces.
- Identificación de los riesgos y de los controles clave de los procesos y de las aplicaciones de gestión significativas.
- Realización de pruebas de recorrido o paso a paso y evaluación del diseño de los controles.
- Realización de pruebas del funcionamiento de los controles clave.
- Realización de procedimientos sustantivos.
- Análisis de los hallazgos, elaboración de las conclusiones y del informe.

Los **objetivos** de la presente Guía de fiscalización del área de compras, gastos y proveedores son ayudar al auditor a:

- Comprender los procedimientos (proceso de gestión) establecidos por la entidad para iniciar, autorizar, registrar, procesar e informar (en las cuentas anuales) de las clases de transacciones significativas relacionadas con la compra de bienes y servicios, desde que se formaliza la necesidad de un usuario, hasta el pago del bien o servicio recibido.
- Identificar y valorar los riesgos de auditoría existentes en el proceso de gestión.
- Comprender los controles que la entidad auditada ha establecido en el proceso de gestión, analizarlos, y determinar cuáles de ellos pueden considerarse controles relevantes o controles clave (los que contribuyen a reducir el riesgo de auditoría).
- Diseñar las pruebas de auditoría más adecuadas para probar la eficacia en el diseño y el funcionamiento de los controles clave.
- Establecer los procedimientos mínimos recomendados para la fiscalización de las áreas de compras, gastos y proveedores/acreedores comerciales, 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 secciones 1310, 1315 y 1330 del MFSC.

2. Ámbito subjetivo de aplicación

Esta guía está diseñada para la fiscalización de empresas y fundaciones públicas que aplican el PGC.

Con los cambios y adaptaciones que en cada caso se requieran, la metodología establecida en esta guía puede ser aplicada en la fiscalización del capítulo 2 de entes públicos con contabilidad presupuestaria.

3. Ámbito objetivo de aplicación

La guía es aplicable a la fiscalización/auditoría de las áreas comprendidas en el ciclo que abarca los procesos de gestión[1] de compras (compra de bienes), gastos (compra de servicios) y proveedores. En particular las cuentas a las que son de aplicación las orientaciones de la presente guía son:

a) Gastos
   - 60 Compras
   - 62 Servicios exteriores
   - 65 Otros gastos de gestión

b) Proveedores y acreedores comerciales
   - 40 Proveedores
   - 41 Acreedores varios

Hay que tener presente que las cuentas de compras y gastos están íntimamente relacionadas con las de proveedores y acreedores, de forma que la evidencia de auditoría que respalde las primeras también sirve para soportar las segundas y viceversa (p.e. si se obtiene evidencia de que se adeuda una factura a un proveedor, esa misma evidencia respalda la cuenta de compras). Por esta razón la planificación y ejecución de la auditoría de estas áreas debe realizarse siempre de forma conjunta y coordinada.

Cuando el alcance de una fiscalización esté limitado a la auditoría de los gastos de explotación, aunque no se diga expresamente se debe entender incluido en ese alcance la auditoría de las cuentas de pasivo relacionadas, sus saldos y movimientos de cargo y abono.

[1] **Definiciones (ver también MFSC-1310):**

Un **proceso de gestión** (proceso de negocio) consiste en una serie de actividades, operaciones o funciones (manuales, semiautomáticas o automatizadas) llevadas a cabo por una entidad, que sirven para llevar a cabo su misión y desarrollar su actividad (la elaboración de productos o el suministro de servicios) o el tratamiento de la información. Un proceso tiene un punto de inicio y otro de finalización claros y generalmente intervienen varios departamentos de la entidad.

Un **subproceso** o función es un subconjunto de actividades o tareas, realizadas por un empleado o funcionario para llevar a cabo una parte de sus responsabilidades, que producen un resultado u output.

Por **procesos de gestión significativos**, a los efectos de la auditoría, se entiende los principales procesos que tienen una influencia directa sobre el flujo de tratamiento contable y la formación o valoración de componentes significativos de las cuentas anuales.

Una **aplicación de gestión** (o aplicación de negocio) es una combinación de hardware y software usada para procesar información de la actividad de la entidad. Puede dar soporte a uno o varios procesos de gestión.

Una **aplicación significativa** a los efectos de la auditoría financiera es aquella que procesa transacciones agregadas superiores al nivel de importancia relativa fijado en la memoria de planificación o si respalda un saldo contable significativo de las cuentas anuales auditadas. El auditor también puede identificar aplicaciones contables como significativas basándose en consideraciones cualitativas. Por ejemplo, sistemas que respaldan la planificación financiera, los informes de gestión y actividades presupuestarias; sistemas que gestionan y proporcionan datos e información de costes; y sistemas que gestionan aspectos relacionados con el cumplimiento de la legalidad (contratación, subvenciones, etc.).

Un **sistema de información financiera** generalmente comprende varias aplicaciones. El sistema de información financiera de la entidad puede ser visto como una serie de agrupamientos lógicos de transacciones y actividades relacionadas y de aplicaciones informáticas. Cada partida presupuestaria o cuenta significativa puede estar afectada o influida por inputs de una o varias aplicaciones (origen de cargos y abonos).

Una **interfaz** es una conexión entre dos dispositivos, aplicaciones o redes, mediante la que se intercambia información. Incluso los entornos ERP (Enterprise Resource Planning) muy integrados a menudo requieren complicadas interfaces para intercambiar información con otras aplicaciones distribuidas.

Un **mapa de procesos** o **flujograma** es una descripción gráfica de las actividades, funciones y procesos de gestión llevados a cabo por la entidad auditada. La descripción incluirá la presencia de los sistemas informáticos utilizados por la entidad para desarrollar su actividad.

El riesgo de incorrección material (**RIM**), es el riesgo de que las cuentas anuales contengan incorrecciones materiales antes de la realización de la auditoría.

4. Objetivos de la auditoría

El objetivo global de auditoría del área de compras, gastos y proveedores consiste en obtener evidencia suficiente y adecuada sobre si las cuentas de compras y gastos relacionadas reflejan de forma razonable el gasto realmente devengado durante el periodo de acuerdo con las normas contables o presupuestarias aplicables y si la gestión se ha realizado de conformidad con la normativa aplicable.

Dicho de otra forma, debemos evaluar si las afirmaciones que subyacen en cada componente o cuenta señalada en el apartado 3 anterior son válidas.

Las afirmaciones son el elemento central para la identificación de los riesgos y de los controles y para seleccionar los procedimientos de auditoría más eficaces en la obtención de esa evidencia.

Los **objetivos** de auditoría para el área de **compras y gastos** (compra de bienes y servicios) relacionados con las **afirmaciones** son:

Objetivos de auditoría del área de Compras y gastos	Afirmaciones[2]
A. Las cuentas de compras y gastos representan los bienes y servicios que han sido adquiridos y recibidos durante el ejercicio, con la debida autorización.	Existencia Integridad Fiabilidad
B. El coste de las mercancías compradas y de los servicios recibidos durante el ejercicio, están debidamente aplicados e imputados contra los ingresos contabilizados en el periodo.	Fiabilidad
C. Los descuentos, bonificaciones, rebajas y otras deducciones de las compras se presentan y clasifican adecuadamente.	Fiabilidad
D. Se presentan y clasifican adecuadamente las transacciones con empresas del grupo, asociadas y partes vinculadas.	Fiabilidad
E. La adquisición de bienes y servicios se ha realizado de acuerdo con lo establecido en la LCSP.	Legalidad
F. Los procedimientos de gestión y las normas de control interno definidas por la dirección son adecuados para asegurar un control efectivo de la gestión de las compras, contabilización y pago, y han funcionado adecuadamente en el periodo auditado[3].	Existencia Integridad Fiabilidad Legalidad

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 compras y gastos que reflejan las cuentas anuales es correcta y si la gestión ha sido conforme con la normativa.

---

[2] MFSC-1315.5: Las afirmaciones ayudan a comprender al auditor los riesgos que se pueden materializar partiendo de la base de que las afirmaciones son las declaraciones que un tercero interesado esperaría encontrar en los estados financieros.

Teniendo en cuenta lo anterior, el auditor debe esperar que la información financiera cumpla con las siguientes afirmaciones dentro la gestión de compras para que la preparación y publicación de información financiera sea confiable y para el cumplimiento con las leyes y normas aplicables.

Afirmación combinada	Afirmación	**Descripción** (afirmaciones relacionadas con los gastos)
Existencia	Acaecimiento (*ocurrencia*)	Las transacciones y hechos registrados han ocurrido y corresponden a la entidad
Integridad	Integridad	Se han registrado todos los hechos y transacciones que tenían que registrarse
Fiabilidad	Exactitud	Las cantidades y otros datos relativos a las transacciones y hechos se han registrado adecuadamente
	Corte de operaciones	Las transacciones y los hechos se han registrado en el período contable correcto
	Clasificación	Las transacciones y los hechos han sido registrados en las cuentas adecuadas
Legalidad	Legalidad	Se ha cumplido la legalidad vigente en la gestión de los gastos.

[3] Ver artículo 58 del RRI de la Sindicatura (MFSC-2).

Los **objetivos** de auditoría para el área de **proveedores y acreedores comerciales**, basados en el Manual de auditoría del REA, y relacionados con las afirmaciones son:

Objetivos de auditoría del área de Proveedores y acreedores comerciales	Afirmaciones relacionadas[4]
A. Los saldos de proveedores y acreedores del balance representan obligaciones reales de la entidad e incluyen facturas pendientes de conformar y pasivos por bienes y servicios recibidos pendientes de facturar.	Existencia Integridad Derechos y obligaciones
B. Las cuentas a pagar están descritas y clasificadas en forma adecuada y las revelaciones necesarias están incluidas en las cuentas anuales y en las notas de la memoria de forma completa y clara	Derechos y obligaciones Valoración

5. Adquirir una comprensión del proceso de gestión

a) Introducción

Para cada una de los tipos de transacciones que son significativos en el contexto de las cuentas anuales y los procesos de gestión relacionados, el auditor debe adquirir un conocimiento suficiente del sistema de información de la entidad para comprender:

- Los procedimientos, tanto manuales como automatizados, mediante los que dichas transacciones son iniciadas, autorizadas, procesadas e incorporadas a las cuentas anuales.
- Cómo se resuelven los procesamientos incorrectos de transacciones.
- Cómo se reconcilian los saldos detallados *(auxiliares)* con el mayor general.
- Los archivos contables relacionados, tanto manuales como digitales (BD); la información soporte; y las cuentas específicas de las cuentas anuales que guardan relación con el inicio, la autorización, y el procesamiento de las transacciones.
- La aplicación informática que soporta el proceso de gestión.

En el caso presente, debemos identificar las clases de transacciones que son significativas para la composición de las cuentas 60/62/65 y 40/41.

En cada entidad habrá ligeras variaciones, de acuerdo con la actividad que desarrollen, pero de una forma u otra son las transacciones relacionadas con la actividad ordinaria de la entidad, las compras o gastos ordinarios y su posterior pago. Esa actividad se desarrolla de acuerdo con determinados procesos de gestión que al realizar la auditoría debemos conocer perfectamente, para identificar dónde puede haber algún riesgo que afecte a las cuentas anuales y centrar nuestras pruebas de auditoría en esos riesgos.

[4] Las afirmaciones ayudan a comprender al auditor los riesgos que se pueden materializar partiendo de la base de que las afirmaciones son las declaraciones que un tercero interesado esperaría encontrar en los estados financieros.

Teniendo en cuenta lo anterior, el auditor debe esperar que la información financiera cumpla con las siguientes afirmaciones sobre los saldos acreedores relacionados para que la preparación y publicación de información financiera sea confiable y para el cumplimiento con las leyes y normas aplicables.

Afirmación	**Descripción** (afirmaciones relacionadas con cuentas de balance)
Existencia	Los activos, pasivos y patrimonio neto existen.
Integridad	La entidad posee o controla los derechos de los activos y los pasivos son obligaciones de la entidad.
Derechos y obligaciones	Se han registrado todos los activos, pasivos e instrumentos de patrimonio neto que tenían que registrarse
Valoración e imputación	Los activos, pasivos y el patrimonio neto se muestran en las cuentas anuales por sus importes adecuados y cualquier ajuste de valoración o imputación resultante está debidamente registrada
Legalidad	Se ha cumplido la legalidad vigente en la gestión de los gastos.

b) Memorándum/narrativa

Para facilitar la adquisición de este conocimiento se puede utilizar el modelo que se adjunta como MFSC-2862.1, pero también puede utilizarse un memorándum o narrativa alternativa a ese modelo que sea lo suficientemente claro y descriptivo.

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 la entidad y un resumen (tan extenso como se considere necesario) en el Archivo Corriente, y estarán adecuadamente referenciados.

Debe entrevistarse a las personas responsables de las distintas tareas y realizar una prueba de recorrido.

En cualquier caso se recomienda vivamente complementarlos con flujogramas y tablas de riesgos y controles como se señala en MFSC-2862.2.

c) Descripción gráfica del proceso de gestión de compras/gastos y proveedores

En una empresa o fundación pública de tamaño mediano o grande, el proceso de gestión de gastos y compras está soportado por una aplicación informática de gestión o por un ERP integrado, que puede abarcar todas las actividades relacionadas, desde la solicitud interna de compra, gestión de la compra, contratación y pedido, recepción de los bienes y servicios adquiridos, autorización de la factura, contabilización y pago.

Se documentará detalladamente la aplicación de gestión utilizada por la entidad.

Para hacer el análisis de los riesgos y controles con mayor precisión conviene disponer cuanto antes de un flujograma del proceso de gestión analizado.

Cuando se trate de ciclos de gestión complejos como el que estamos estudiando, se empezará dibujando el mapa del proceso o flujograma general, señalando los principales subprocesos o funciones que posteriormente se han de describir con mayor detalle, tal como se describe en MFSC-2862.2.

d) Identificar las aplicaciones de gestión y las interfaces

En esta fase se podrá contar con la colaboración de la UASI.

6. Identificación de los riesgos del proceso de gestión y de los controles existentes.

Al analizar el proceso, en primer lugar, se deben identificar los riesgos existentes en cada fase, valorar los riesgos de incorrecciones materiales (RIM) y posteriormente identificar los controles internos que ha implantado la entidad para mitigarlos.

Cuando se aborda el análisis de los riesgos de un determinado ciclo o proceso de gestión el enfoque principal consiste en responder, tanto con carácter general, como en cada uno de los subprocesos analizados, a la pregunta:

¿Qué puede ir mal

en el proceso de gestión 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 en las CCAA?.

Se debe realizar o discutir este análisis en equipo siguiendo MFSC-1315.4. Se deben repetir estas preguntas en cada una de las etapas del proceso.

Por ejemplo, podría suceder:

- Que se paguen cantidades por compras o servicios no recibidos
- Tramitación de pedidos/compras no autorizados y consecuentes pagos indebidos
- Albaranes de recepción incorrectos
- Tramitación y pago de facturas incorrectas o no autorizadas
- Pagos, por compras/servicios recibidos, a cuentas que no son las del proveedor.

La lista puede hacerse, en cada caso, tan larga como se desee. Para facilitar el trabajo se pueden establecer listas previas sistematizadas y ordenadas por las principales funciones, como la del siguiente cuadro, en la que

se señalan algunos de los principales riesgos inherentes a cada función o subproceso y el objetivo de control correspondiente.

Funciones	Ejemplos de riesgos inherentes	Objetivo de control interno
Mantenimiento del Maestro de proveedores	• Cambios erróneos o no autorizados en el fichero maestro.	Todos los cambios en el FMP deben estar debidamente autorizados.
Formulación de las solicitudes de compra	• Compras en condiciones desfavorables a proveedores no autorizados.	Las solicitudes de mercancías y servicios las inician y aprueban personas autorizadas.
Gestión de compras	• Compras no autorizadas. • Compra de cantidades superiores a las necesarias o de calidad deficiente.	Todos los pedidos de compra se basan en solicitudes válidas y debidamente aprobadas y se ejecutan correctamente en cuanto a precio, cantidad, calidad y proveedor.
Recepción de bienes y servicios	• Recepción de materiales o servicios no adquiridos o solicitados debidamente. • No se informa sobre las mercancías dañadas o no recibidas.	Todos los materiales y servicios recibidos concuerdan con los pedidos originales.
Tramitación de las facturas (comprobación)	• Aceptación de facturas por materiales o servicios no recibidos, o con precios o condiciones incorrectos. • Las cuentas no reflejan las operaciones correctamente.	Todas las facturas procesadas para su pago corresponden a mercancías y servicios recibidos y son exactas en lo que se refiere a condiciones, cantidades, precios y cálculos. La clasificación en cuentas es correcta y concuerda con el plan de cuentas.
Gestión de pagos	• Pagos incorrectos o duplicados. • Alteración de los cheques. • Pago de materiales o servicios no recibidos.	Todos los pagos se preparan basándose en documentos y debidamente aprobados, se cotejan con los datos justificativos, se aprueban debidamente, se firman y se envían por correo o se transfieren los fondos.
Contabilidad	• Saldos incorrectos en el mayor general de las cuentas relacionadas. • Cuentas anuales incorrectas.	Todas las facturas y pagos se registran pronta y exactamente en cuanto a su beneficiario e importe. Todos los asientos en las cuentas por pagar, de gastos y de pagos se acumulan, clasifican y resumen adecuadamente en las cuentas.

En TeamStore se va a crear un repositorio de riesgos, controles y pruebas de auditoría relacionadas.

Tras el dibujo de los flujogramas y la identificación de los riesgos y controles existentes, estos se recogerán en unas tablas tal como se describe en ***MFSC-2862.2 Descripción del proceso de gestión de compras, gastos y proveedores.***

En esas tablas se relacionarán riesgos identificados con los objetivos de control y con las actividades de control. El objetivo es identificar y obtener la comprensión de las actividades de control que hacen frente de forma eficaz a las áreas en las que los RIM tienen mayores probabilidades de suceder.

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

Se debe determinar 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 indicativo de debilidad del control interno.

7. Segregación de funciones

Al revisar un proceso de gestión, 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.

En la práctica, este principio de segregación de las funciones 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.

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[5].

En los actuales sistemas ERP, 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", en los sistemas de información actuales el análisis de la segregación de funciones **solo es posible realizarlo** con técnicas de auditoría de sistemas por personal especializado.

En MFSC-2862.3 se recogen las principales situaciones de falta de segregación de funciones en las operaciones de compra, recepción, contabilización de cuentas por pagar y pagos, que pueden entrañar riesgos de errores o irregularidades, y por tanto riesgos de auditoría.

8. Identificación y revisión de las interfaces

Las interfaces son programas que sirven para transferir datos de una aplicación a otra.

Por ejemplo, una empresa utiliza una aplicación para gestionar las compras y semanalmente traspasa toda la información de las adquisiciones a la aplicación de contabilidad. El programa que se utiliza para hacer la transferencia de datos es la interfaz entre compras y contabilidad.

Otro caso frecuente es aquel en que una empresa gestiona sus compras y relaciones con los proveedores con una aplicación y periódicamente transfiere los datos de los pagos a realizar a un programa de gestión de tesorería.

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.
c) Diseñar y ejecutar las pruebas de auditoría que se estimen pertinentes para garantizar la exactitud e integridad de los datos.
d) Pueden identificarse deficiencias de control como las de los siguientes ejemplos extraídos de nuestros informes:

Deficiencia de control observada	Riesgo	Recomendación
Una vez efectuada la conciliación entre facturas y pagos a tramitar, a través de SAP se genera un fichero de transferencias, con el formato establecido, para el envío a la entidad bancaria para proceder al pago. Se ha verificado que el fichero generado por SAP es editable y podría ser modificado previamente al envío a la entidad financiera, lo que representa un riesgo sobre la integridad y autenticidad de la información.	**Bajo**	Establecer un control de conciliación del detalle de los pagos tramitados por la entidad financiera y los remitidos por la entidad.

[5] Un **control compensatorio** es aquel que reduce el riesgo de una debilidad, real o potencial, existente en otro control.

9. Evaluación de los CGTI: Factores de riesgo a considerar

Hay determinados controles de los procesos/aplicaciones cuya eficacia depende en una medida importante en el buen funcionamiento de los controles generales.

Por tanto, la revisión de los controles de aplicación y la decisión de depositar confianza en ellos debe hacerse tras una evaluación positiva de los controles generales de tecnologías de la información (CGTI), tanto de los existentes a nivel de entidad y sistemas TI como a nivel de los procesos/aplicaciones de compras, según los procedimientos descritos en MFSC-2850 y siguientes.

La **UASI** al realizar la revisión de los CGTI tendrá en cuenta, en particular, pero no exclusivamente, los siguientes riesgos existentes en el nivel de la aplicación informática de gestión auditada.

Entorno de control

Un entorno de control efectivo es fundamental para asegurar que la información sobre compras y el tratamiento de dicha información sean exactos y completos, y que se mantengan la integridad y confidencialidad de la información.

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 se detallan a lo largo del presente informe, que ponen en cuestión la eficacia del sistema de control interno de la Fundación 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. La forma en que la alta dirección expresa sus convicciones respecto de la importancia del control interno y determina en gran medida su eficacia. Aunque la fundación dispone de algunos sistemas potencialmente eficaces (una aplicación informática de gestión potente, un servicio de control interno, normas de gestión, etc) en el curso de la fiscalización se ha puesto de manifiesto que su implantación presenta una serie de deficiencias de carácter significativo que convierte a aquellos en parcialmente, o en algunos casos en gran medida, ineficaces para el logro de los objetivos de control.	**Alto** Debido a las circunstancias indicadas no se puede tener la seguridad de que todos los gastos efectivamente realizados 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.	Se recomienda a los órganos de dirección que establezcan, formalicen, comuniquen, mantengan operativos y exijan su cumplimientos, 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.

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 deberá evitar que se introduzcan sin la autorización apropiada modificaciones en la información sobre los maestros de proveedores o de productos, o en la aplicación que gestiona las compras, etc. Contemplará entre otras cuestiones que:

- Todas las solicitudes de cambios a introducir en las aplicaciones de gestión de comprs, 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 autorizarse antes de ser introducidos en el entorno de producción.
- Debe existir separación de funciones a fin de limitar la capacidad del personal para realizar cambios que afecten tanto a la base de datos de producción como a la configuración de la aplicación de compras.

Si una aplicación se ha desarrollado en la entidad y un equipo de desarrolladores internos tiene acceso a modificar la aplicación, el riesgo asociado será alto. 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 compras y a los aspectos fundamentales de sus operaciones, el mantenimiento y las **actualizaciones** de las aplicaciones deberían ser incorporados al proceso de gestión de cambios.

Algunos ejemplos extraídos de nuestros informes:

Deficiencia de control observada	Riesgo	Recomendación
5º No existe segregación de funciones en el acceso y transporte a producción. Los mismos desarrolladores y un usuario de negocio que llevan a cabo las modificaciones, son los encargados de realizar los transportes a producción de los cambios realizados y tienen acceso al entorno de producción como usuarios privilegiados. El acceso para realizar transportes por parte de los desarrolladores es altamente desaconsejable (especialmente si son proveedores externos), ya que no garantiza una adecuada segregación de funciones, permitiendo realizar transportes de forma no controlada. En este caso, tampoco existen controles compensatorios que mitiguen el riesgo existente.	**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 debidas a errores o irregularidades.	Se recomienda establecer una adecuada segregación de funciones en los traspasos al entorno productivo. La capacidad de realizar los traspasos al entorno productivo debería estar restringida a personal que no tenga acceso al entorno de desarrollo. En caso de no ser posible establecer esa segregación de tareas, deberían implementarse controles compensatorios adicionales como por ejemplo: - Realizar revisiones periódicas de los transportes efectuados, que garanticen que únicamente se han llevado a cabo aquellos transportes por cambios autorizados. - Incorporar avisos automáticos a los responsables cada vez que se realice un transporte, para garantizar que ningún transporte pase inadvertido. - Inhabilitar el acceso a producción de los desarrolladores y habilitarlo de forma autorizada bajo demanda cada vez que requieran realizar un transporte a producción. La implementación de controles compensatorios mitigaría el riesgo de que puedan realizarse transportes a producción de forma no autorizada.

Controles de accesos y de usuarios

Los riesgos de acceso se centran en los riesgos asociados con accesos indebidos a los sistemas, a los datos y a la información financiera o contable.

Abarca los riesgos asociados a una indebida segregación de funciones, la integridad de la información y bases de datos contables y la confidencialidad de la información.

Una gestión eficaz de los controles de acceso de los usuarios proporciona garantía de que los sistemas de gestión de compras están adecuadamente protegidos para evitar el uso no autorizado, divulgación, modificación o pérdida de información. La gestión de usuarios es también un componente crítico para el establecimiento de una efectiva separación de funciones.

Los parámetros críticos que pueden incidir en los accesos a las aplicaciones contables son:

Número de usuarios

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, de que existan conflictos por accesos incompatibles o por una monitorización inadecuada de los accesos.

Privilegios

El acceso o la modificación de los privilegios de acceso deben ser aprobados y documentados.

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.

Acceso directo a la Base de Datos (BD) subyacente

Este es un parámetro crítico, ya que puede dejar puertas traseras para acceder a las BD.

Pocas aplicaciones guardan los datos en la misma aplicación e impiden el acceso directo a los datos. Sin embargo algunas aplicaciones permiten a los usuarios acceder directamente a la BD sin necesidad utilizar la aplicación. En este último caso el riesgo será superior.

Autenticación integrada o independiente

Los usuarios del sistema de gestión de compras 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.

Si una aplicación integra la autenticación con el sistema operativa (SO) el riesgo es alto porque los usuarios autorizados para gestionar el SO pueden acceder también a la aplicación, pero si la aplicación tiene sus propios mecanismos de autenticación, el riesgo será inferior porque una persona con permisos totales en el SO, un administrador, necesitará también estar autorizado e identificarse para acceder a la aplicación.

Veamos algunos ejemplos extraídos de nuestros informes:

Deficiencia de control observada	Riesgo	Recomendación
3º En relación con las políticas de seguridad, se ha observado que las directivas de **contraseñas** no son todo lo robustas que sería conveniente de acuerdo con las mejores prácticas en la materia. La deficiencia de control, que afecta a todos los niveles del sistema de información (SAP, Oracle, HP-UX, Directorio activo), nos ha permitido constatar intervalos de caducidad elevados, desbloqueo automático de cuenta en caso de superar los intentos de acceso fallido prefijados, periodo de tiempo elevado en el cierre de sesión por inactividad, no activación de requerimientos de complejidad de las contraseñas, elevado número de usuarios cuya contraseña no caduca, así como usuarios que no requieren de contraseña para acceder al entorno.	**Alto** Las deficiencias detectadas debilitan la efectividad del control de acceso en los distintos niveles de los sistemas de información representando un riesgo (valorado como medio) de manipulación indebida de los datos para su consulta o alteración, así como supone un riesgo sobre la integridad y confidencialidad de los datos de la Entidad.	Recomendamos 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).
10ºLos 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 representa 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. En el curso de la realización del presente Informe se han reducido de forma importante dichos permisos (un 63%), pasando de 16 a 6, mitigando el riesgo existente a una valoración de medio al cierre del ejercicio, pero el número y tipo de usuario todavía se considera excesivo.	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
11ºEn el entono SAP se ha detectado un número excesivo de usuarios con acceso a transacciones críticas de sistemas, como pueda ser el mantenimiento de usuarios o la actualización directa de tablas. El acceso a funcionalidades críticas del sistema, así como las debilidades en la configuración de seguridad durante el ejercicio representaba un alto riesgo de acceso indebido a la información existente en el entorno suponiendo una	**Alto** En el curso de la realización del presente Informe se han reducido de forma importante (un 83%) los usuarios con accesos privilegiados, pasando de una media de usuarios por transacción analizada de 30 a 5, mitigando el riesgo existente, pero el número y tipo de usuario restante todavía se considera excesivo.	Se recomienda revisar los accesos a las transacciones críticas de SAP asociados a TI y evaluar la idoneidad de dichos accesos, eliminando el permiso a aquellos usuarios que no lo necesiten para el desempeño de sus tareas. Adicionalmente se recomienda realizar revisiones formales y periódicas (al menos de forma anual) de los permisos asignados a los usuarios, especialmente con el objeto de detectar accesos no autorizados a transacciones críticas. En estas

Deficiencia de control observada	Riesgo	Recomendación
amenaza para la integridad y confidencialidad de la información.		revisiones debería participar tanto el área de sistemas como el área de negocio.
10º 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, usuarios con nombres genéricos y usuarios a los que no se les aplican las políticas de contraseñas.	**Medio** Esta situación implica un riesgo medio de accesos indebidos y de actuaciones no autorizadas.	Recomendamos la formalización de 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 realización periódica de revisiones de los usuarios autorizados y los permisos asignados en los sistemas y aplicaciones, de forma que se garantice que cada usuario dispone de las capacidades mínimas necesarias para desempeñar sus tareas y ninguna más. Debe conservarse la documentación acreditativa de la realización de las revisiones, los resultados y las acciones llevadas a cabo.
1º Se han identificado un total de 6.372 usuarios con acceso a la aplicación de compras, de los cuales 1.127 (17,7%) son usuarios inactivos desde hace más de 6 meses, y 591 (9,3%) no han accedido nunca a la aplicación. También existen 47 usuarios genéricos (0,7% sobre el total). En 2013 ha finalizado la implantación de la aplicación, por lo que se han dado de alta 2.335 nuevos usuarios y se han dado de baja 122 usuarios. Hemos seleccionado una muestra de 25 altas y 10 bajas y se han solicitado las evidencias asociadas al proceso de gestión de usuarios. No ha sido posible, en todos los casos, obtener evidencias de que dicho proceso se lleve a cabo de manera formalizada.	**Medio** La situación descrita representa un riesgo valorado como medio de que se produzcan accesos no autorizados a la aplicación, utilizando algún usuario inactivo.	Recomendamos formalizar de 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. También debe incluir la realización de revisiones periódicas de los usuarios autorizados y los permisos asignados en los sistemas y aplicaciones, de forma que se garantice que cada usuario dispone de las capacidades mínimas necesarias para desempeñar sus tareas y ninguna más. Debe conservarse la documentación acreditativa de las revisiones realizadas, los resultados y las acciones llevadas a cabo. De acuerdo con la información facilitada, la entidad ha implantado con posterioridad a la finalización del trabajo de campo un procedimiento de revisión periódica semestral de usuarios obsoletos que contempla eliminar los usuarios inactivos durante más de seis meses.
Al revisar la gestión de usuarios, se han identificado múltiples usuarios genéricos o indeterminados.	Esta circunstancia supone un riesgo **alto** de accesos no autorizados a las aplicaciones y al dominio, y la imposibilidad de atribuir responsabilidades y de garantizar una adecuada segregación de funciones en los procesos de gestión.	Recomendamos eliminar los usuarios genéricos, transformándolos a usuarios nominativos y, en caso de necesitar utilizarlos excepcionalmente, asignar la responsabilidad sobre dicho usuario genérico a alguna persona determinada.

Continuidad del servicio

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

- Se debe disponer de una estrategia documentada para la gestión de las copias de seguridad periódicas, tanto de los datos como de los programas de gestión de compras; y
- Hay que definir los plazos de retención y los requisitos de almacenamiento para la información.

Algunos ejemplos extraídos de nuestros informes:

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	En caso de ocurrir un desastre que afectase al CPD, existe el riesgo alto de que se pierdan, de forma irreversible, los sistemas de producción junto con las	Debe desarrollarse un plan de gestión de la continuidad del servicio, que contemple, en sentido amplio, todos los activos que dan soporte a sus procesos (personas, instalaciones, proveedores, sistemas de información,

Deficiencia de control observada	Riesgo	Recomendación
mismo CPD.	configuraciones de los sistemas y la lógica de las aplicaciones. La reconstrucción de esta pérdida (las principales aplicaciones de la Entidad) podría prolongarse durante meses.	etc.), sus requisitos de disponibilidad, el desarrollo de los correspondientes planes de recuperación en caso de ocurrencia de una contingencia grave que afecte a su disponibilidad, así como los mecanismos orientados a garantizar la validez de dichos planes de manera continuada en el tiempo.
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.	Recomendamos el traslado y ubicación fuera del CPD de las copias de seguridad que se realicen de datos y programas.
No se ha definido un plan de continuidad de la actividad que permita la recuperación de los procesos de gestión críticos, tras la ocurrencia de una contingencia que afecte a los sistemas de producción, en un tiempo limitado y fijado con anterioridad.	Existe un riesgo **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.	Recomendamos elaborar y aprobar un plan de recuperación de la actividad, basado en un análisis de riesgos y en la identificación de los activos de TI que son críticos para la entidad, detallando las tareas a realizar para restablecer el servicio, los plazos máximos de respuesta y los periodos de retención de la información.

10. Procedimientos de Auditoría

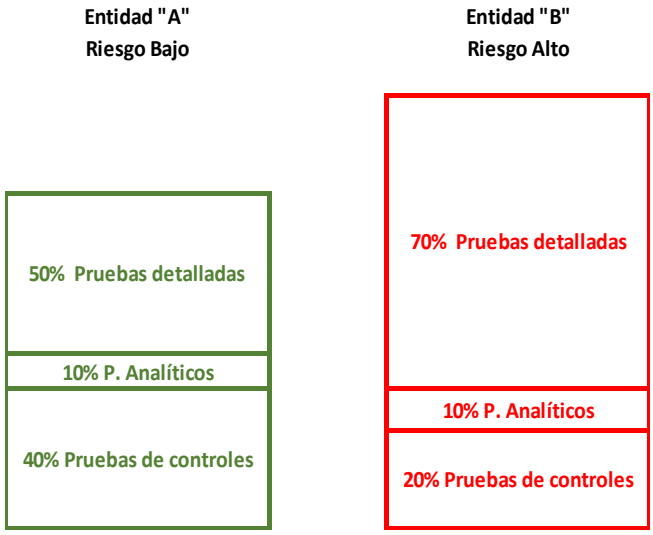
La naturaleza, momento y alcance de los procedimientos de auditoría se determinan de acuerdo con las circunstancias de cada trabajo y deben basarse en el conocimiento de la actividad que realiza el ente auditado, de su organización, de los riesgos valorados así como en la evaluación del control interno 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)

Podemos ver con un ejemplo gráfico como puede variar la cantidad (suficiencia) de evidencia necesaria en relación con la “Tesorería” y los tipos de pruebas necesarias para obtenerla



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

- Se debe evaluar la gravedad de dichas deficiencias

- Modificar la valoración preliminar del riesgo
- Documentar las implicaciones de las deficiencias de control.

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

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

Los procedimientos de auditoría relacionados con las áreas de compras, gastos y proveedores (los contemplados en esta guía están en negrita) son:

- Adquisición de un conocimiento de los procesos de gestión significativos. (MFSC-2862.1).
- Identificación de las aplicaciones informáticas de gestión significativas (las que soportan los procesos de gestión significativos) y de las principales interfaces. (MFSC-2862.1).
- Documentar la comprensión del proceso de gestión (MFSC-2862.1).
- Dibujar un flujograma del proceso completo (MFSC-2862.2).
- Revisar las conclusiones de la revisión de los CGTI relacionados con el proceso de gestión auditado.
- Identificación de los riesgos y de los controles clave de los procesos y aplicaciones de gestión significativas (MFSC-2862.2).
- Realización de pruebas de recorrido o paso a paso y evaluación de la eficacia del diseño de los controles.
- Realización de pruebas del funcionamiento de los controles clave (pruebas de cumplimiento).
- Procedimientos sustantivos.

  Deben incluir la inspección de los documentos, investigación y comentarios con el personal del cliente y la confirmación directa de los proveedores y acreedores. Resulta de gran utilidad la evaluación general de los saldos, incluyendo las relaciones que existen entre cuentas a pagar y compras de materiales y servicios.

En los anexos *MFSC-2862.4 Programa de auditoría de compras y gastos* y *MFSC-2862.5 Programa de auditoría de proveedores* se incluyen los programas de trabajo estándar que deben adaptarse a las circunstancias de cada fiscalización.

Dichos programas están disponibles en el sistema de papeles de trabajo electrónico de la Sindicatura (TeamStores) y son actualizados periódicamente.

11. Colaboración UASI

La realización de algunos de los procedimientos de auditoría descritos en esta guía, requerirán la colaboración de la UASI con el equipo de fiscalización encargado en trabajo. Con esa finalidad el Auditor responsable se pondrá en contacto con el Jefe de la UASI al iniciar la planificación del trabajo para coordinar la colaboración.

12. Aplicación de esta guía

Esta guía se aplicará en las fiscalizaciones de nivel de control general o cuando esté previsto fiscalizar el área de personal.

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

Anexos:

Sección MFSC-2862.1:	Documentar la comprensión del proceso de gestión
Sección MFSC-2862.2:	Descripción del proceso de gestión de compras, gastos y proveedores
Sección MFSC-2862.3:	Segregación de funciones en compras, gastos y proveedores
Sección MFSC-2862.4:	Programa de auditoría de compras y gastos
Sección MFSC-2862.5:	Programa de auditoría de proveedores

Sección MFSC-2862.10 Principales deficiencias de control interno referidas a compras de los informes de la Sindicatura