Guía práctica de fiscalización de los OCEX

GPF-OCEX 1962 Guía de auditoría del área de compras de bienes y servicios

Referencia: GPF-OCEX 1315 Revisada y GPF-OCEX 1316 Revisada

Documento elaborado por la Comisión Técnica de los OCEX y
aprobado por la Conferencia de Presidentes de ASOCEX el 19/10/2023.

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.

El gasto en compras de bienes y servicios de una entidad es el resultado de la agregación de un gran número de transacciones de importes relativamente poco significativos, que de ordinario se gestionan con sistemas de información complejos y cada vez más automatizados e integrados. En estas situaciones, especialmente en las entidades **de tamaño mediano o grande, llegar a una conclusión de auditoría (favorable o desfavorable) sólo con pruebas sustantivas es, en la práctica, imposible**, siendo preciso confiar en los controles internos, automatizados en su mayor parte o TI dependientes, existentes en los procesos/aplicaciones de gestión que ha diseñado e implantado la entidad y, por tanto, deben hacerse pruebas de auditoría sobre el diseño, implementación y eficaz funcionamiento de estos.

La adecuada comprensión de esta guía **requiere el conocimiento previo de las GPF-OCEX 1315R, 1316R, 5330 y 5340.**

Los **objetivos** de esta Guía de auditoría del área de compras, gastos y proveedores son ayudar al auditor a:

- Conocer los **procedimientos/procesos 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 inherentes** existentes en las afirmaciones.
- Conocer los **controles** que la entidad auditada ha establecido en el proceso de gestión, analizarlos, y determinar cuáles de ellos responden a los riesgos inherentes en las afirmaciones.
- Diseñar las **pruebas de auditoría** más adecuadas para probar la eficacia en el diseño e implementación y probar el funcionamiento operativo de los controles.
- 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.

2. Ámbito subjetivo de aplicación

Esta guía está diseñada para la fiscalización de empresas, fundaciones públicas y otras entidades del sector público 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 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:

De carácter financiero:

a) Gastos

60 Compras
62 Servicios exteriores
65 Otros gastos de gestión

b) Proveedores y acreedores comerciales

40 Proveedores
41 Acreedores varios

De carácter presupuestario:

a) Capítulo 2 Gastos corrientes en bienes y servicios

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.

4. Objetivos de la auditoría

El objetivo general de la 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:

	Afirmación	Descripción/Objetivo
Afirmaciones sobre tipos de transacciones y hechos (*los gastos por compras de bienes y servicios*) y la correspondiente información a revelar, durante el periodo	**Ocurrencia**	Los gastos por compras de bienes y servicios contabilizados o revelados han ocurrido y dichas transacciones y hechos corresponden a la entidad.
	Completitud	Se han contabilizado todos los gastos por compras de bienes y servicios que tenían que registrarse y se ha incluido toda la información a revelar relacionada que se tenía que incluir en los estados financieros
	Exactitud	Las cantidades y otros datos relativos a los gastos por compras de bienes y servicios se han contabilizado adecuadamente y la correspondiente información a revelar ha sido adecuadamente medida y descrita.
	Corte de operaciones	Los gastos por compras de bienes y servicios se han contabilizado en el periodo correcto.
	Clasificación	Los gastos por compras de bienes y servicios se han contabilizado en las cuentas apropiadas.
	Presentación	Los gastos por compras de bienes y servicios han sido adecuadamente agregados o desagregados y están descritos con claridad y la correspondiente información a revelar es pertinente y comprensible en el contexto de los requerimientos del marco de información financiera aplicable.
	Legalidad	Se ha cumplido la legalidad vigente en la gestión de los gastos por compras de bienes y servicios.

Los **objetivos** de auditoría para el área de **acreedores relacionados con los gastos por compras de bienes y servicios** son:

	Afirmación	Descripción/Objetivo
Afirmaciones sobre los acreedores por gastos por compras de bienes y servicios y la correspondiente información a revelar, al cierre del periodo	**Existencia**	Los acreedores por gastos por compras de bienes y servicios de pago existen.
	Derechos y obligaciones	Los pasivos por acreedores por gastos por compras de bienes y servicios de pago son obligaciones de la entidad.
	Completitud	Se han contabilizado todos los acreedores por gastos por compras de bienes y servicios pendientes de pago que tenían que registrarse y se ha incluido toda la información a revelar relacionada que se tenía que incluir en los estados financieros.
	Exactitud, valoración e imputación	Los pasivos figuran en los estados financieros por los importes adecuados y cualquier ajuste resultante a la valoración o imputación ha sido adecuadamente contabilizado, y la correspondiente información a revelar ha sido adecuadamente medida y descrita.
	Clasificación	Los pasivos se han contabilizado en las cuentas apropiadas.
	Presentación	Los pasivos han sido adecuadamente agregados o desagregados y están descritos con claridad y la correspondiente información a revelar es pertinente y comprensible en el contexto de los requerimientos del marco de información financiera aplicable.

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.

5. Obtención de conocimiento del proceso de gestión

De acuerdo con el apartado 25 de la GPF-OCEX 1315R y 28 de la GPF-OCEX 1316R, el auditor debe obtener conocimiento del sistema de información y comunicación (SIC) de la entidad que sea relevante para la preparación de los estados financieros y los gastos por compras de bienes y servicios en este caso, mediante la aplicación de procedimientos de valoración del riesgo a través del conocimiento de las actividades de procesamiento de la información de la entidad, incluidos sus datos e información, los recursos que se deben utilizar en esas actividades y las políticas que definen, para los gastos por compras de bienes y servicios:

i. el modo en que la información fluye por el sistema de información de la entidad, incluido el modo en que:
    a. las transacciones se inician y la información sobre ellas se registra, se procesa, se corrige si es necesario, se traslada al mayor y se incluye en los estados financieros; y
    b. la información sobre los hechos y condiciones, distintos de las transacciones, se captura, se procesa y se revela en los estados financieros;
ii. 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;
iii. el proceso de información financiera utilizado para la preparación de los estados financieros de la entidad, incluida la información a revelar; y
iv. los recursos de la entidad, incluido el entorno de TI, relevantes para los apartados i a iii anteriores (la aplicación informática que soporta el proceso de gestión de compras y las interfaces existentes, entre otras cuestiones).

Memorándum/narrativa

Aunque en cada entidad habrá ligeras variaciones, básicamente nos interesa conocer el proceso de gestión de compras desde que surge la necesidad hasta su pago. Debemos conocerlos de forma clara para identificar dónde puede haber algún riesgo que afecte a las cuentas anuales o al cumplimiento de la legalidad y así poder centrar nuestras pruebas de auditoría en esos riesgos.

Para adquirir ese conocimiento y documentarlo, 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 nuestro conocimiento de los procedimientos aplicados es correcto, es decir, que la descripción se corresponde con los procedimientos ejecutados en la práctica por la entidad.

Para facilitar la adquisición del conocimiento de los procedimientos de gestión se puede utilizar el formulario modelo que se adjunta en el Anexo 1, pero también pueden utilizarse memorándums o narrativas 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.

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 detallado del proceso de gestión analizado (véase GPF-OCEX 1512).

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.

Para identificar las aplicaciones de gestión y las interfaces existentes (fundamentalmente con contabilidad y con el sistema de pagos) se podrá contar con la colaboración de expertos en auditoría de sistemas de información. Se documentará detalladamente la aplicación de gestión utilizada por la entidad.

6. Identificación y valoración de los riesgos inherentes en las afirmaciones e identificación de los controles de procesamiento de la información.

Al analizar el proceso se deben identificar los riesgos inherentes en las afirmaciones existentes en cada fase del proceso, valorar los riesgos de incorrecciones materiales (RIM), elaborar el espectro de riesgo inherente[1] y determinar aquellos riesgos que se considerarán significativos (los que se encuentran próximos al límite superior del espectro de riesgo inherente).

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

Cuando se aborda el análisis de los riesgos de un 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 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.

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 de riesgos potenciales 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 de la siguiente **tabla**, en la que se señalan algunos de los principales riesgos inherentes a cada función o subproceso y el objetivo de control correspondiente.

[1] Ver GPF-OCEX 1315R y GPF-OCEX 1316R (apartado 50 y siguientes).

Tabla de valoración de los riesgos inherentes en las afirmaciones

Funciones	Ejemplos de riesgos inherentes	Afirmación	Proba-bilidad (1 a 10)	Magnitud (1 a 10)	Valoración del R.I. (PxM)	Objetivo de control interno
Mantenimiento del FMP	R211 Cambios erróneos o no autorizados en el fichero maestro de proveedores (FMP).					Todos los cambios en el FMP deben estar debidamente autorizados.
Formulación de las solicitudes de compra	R221 Compras en condiciones desfavorables a proveedores no autorizados.					Las solicitudes de mercancías y servicios las inician y aprueban personas autorizadas.
Gestión de compras	R231 Compras no autorizadas. R232 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	R241 Recepción de materiales o servicios no adquiridos o solicitados debidamente. R242 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)	R251 Aceptación de facturas por materiales o servicios no recibidos, o con precios o condiciones incorrectos. R252 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	R261 Pagos incorrectos o duplicados. R262 Alteración de los cheques. R263 Pago de materiales o servicios no recibidos.					Todos los pagos se preparan basándose en documentos debidamente aprobados, se cotejan con los datos justificativos, se aprueban debidamente, se firman y se transfieren los fondos (o se envían por correo en caso de cheques o pagarés).
Contabilidad	R271 Saldos incorrectos en el mayor general de las cuentas relacionadas. R272 Cuentas anuales incorrectas.					Todas las facturas y pagos se registran con prontitud y exactamente en cuanto a su beneficiario e importe. Todos los asientos en las cuentas por pagar, de gastos y de tesorería se acumulan, clasifican y resumen adecuadamente en las cuentas anuales.

Tras la narrativa, el dibujo de los flujogramas y la identificación de los riesgos inherentes existentes, estos se recogerán en unas tablas que relacionen los riesgos identificados con los objetivos de control y con los controles relevantes, con objeto de identificar y obtener una mejor 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.

El auditor determinará si los procedimientos sustantivos por sí solos no pueden proporcionar evidencia de auditoría suficiente y adecuada con respecto a alguno de los riesgos significativos en las afirmaciones.

Cuando transacciones rutinarias estén sujetas a un procesamiento muy automatizado con escasa o nula intervención manual, puede que no resulte posible aplicar únicamente procedimientos sustantivos en relación con el riesgo. 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 (por ejemplo, en los procesos de nómina en una entidad mediana o grande).

En estas circunstancias, la única forma de obtener evidencia de auditoría suficiente y adecuada es comprobar la eficacia operativa de los controles existentes.

En consecuencia, se requiere que el auditor **identifique** los controles de procesamiento de la información (CPI) que ha implantado la entidad para mitigar los riesgos inherentes identificados y **valore el riesgo de control** por las implicaciones para el diseño y aplicación de procedimientos posteriores de auditoría de conformidad con la NIA-ES-SP 1330 para responder a los RIM en las afirmaciones.

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

Hay determinados controles de procesamiento de la información (CPI) cuya eficacia depende en gran medida del buen funcionamiento de los controles generales.

Por tanto, la revisión de los CPI y la decisión de depositar confianza en ellos debe hacerse tras una evaluación previa 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 gestión de compras, según los procedimientos descritos en la GPF-OCEX 5330.

Al realizar la revisión de los CGTI se pueden tener en cuenta, a modo de ejemplo, los siguientes riesgos derivados de la utilización de las TI.

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 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	**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 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.

Deficiencia de control observada	Riesgo	Recomendación
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.		

Dentro de este apartado es importante considerar si existe una adecuada planificación de necesidades y de compras, con la finalidad de obtener las mejores condiciones que permita el mercado.

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 compras, 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 informes de fiscalización:

Deficiencia de control observada	Riesgo	Recomendación
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.

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 operativo (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:

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	**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).

Deficiencia de control observada	Riesgo	Recomendación
usuarios que no requieren de contraseña para acceder al entorno.		
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 amenaza para la integridad y confidencialidad de la información.	**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 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.

Deficiencia de control observada	Riesgo	Recomendación
		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:

Deficiencia de control observada	Riesgo	Recomendación
Aunque se dispone de una arquitectura de alta disponibilidad para los servidores de aplicación basada en la existencia de clústeres de servidores, todos los equipos se ubican en un mismo CPD.	En caso de ocurrir un desastre que afectase al CPD, existe el riesgo 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 (las principales aplicaciones de la Entidad) podría prolongarse durante meses.	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, 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.

8. Revisión de los controles de procesamiento de la información (CPI)

El **objetivo de la auditoria de los CPI** será obtener una seguridad razonable de que el sistema de control interno garantiza la completitud, exactitud, validez y legalidad de las transacciones y datos registrados en la aplicación de gestión revisada y su posterior contabilización; es decir, si la eficacia de los CPI garantiza la correcta ejecución de los procesos de gestión auditados y mitigan el riesgo de errores e irregularidades.

Los CPI son procedimientos manuales o automatizados que operan a nivel de procesos de gestión y que se aplican al procesamiento de las transacciones mediante aplicaciones informáticas específicas. Estos controles se extienden sobre el conjunto del proceso de gestión o actividad cubierto por la aplicación de gestión. **Su comprobación proporcionará confianza únicamente sobre aquellas clases de transacciones concretas procesadas por esa aplicación, ya que son controles específicos y únicos para cada proceso de gestión.**

9. 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 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.

Para analizar si existe una adecuada segregación de funciones incompatibles, tanto en sistemas informatizados como no, es importante obtener respuesta a los siguientes tipos de preguntas:

¿Las responsabilidades de las funciones de formulación de solicitudes de compra, compras y recepción, están segregadas de las funciones de tramitación de facturas, cuentas por pagar y contabilidad?

¿Las responsabilidades de la función de compras están segregadas de las actividades de formulación de solicitudes de compra y recepción?

¿Las responsabilidades de las funciones de tramitación de facturas y de cuentas por pagar están segregadas de la función de contabilidad?

¿Las responsabilidades de las funciones de preparación y aprobación de los pagos están segregadas de las funciones de contabilización de los pagos y de contabilidad?

¿Las responsabilidades de la función de aprobación de los pagos están segregadas de las responsabilidades de la función de preparación de los mismos?

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**[2] que ayuden a mitigar la gravedad de las debilidades de control.

Procedimientos de auditoría

Para facilitar la revisión, en el cuadro siguiente se recogen las principales situaciones de falta de segregación de funciones en el proceso de gestión de compras que pueden entrañar riesgos de errores o irregularidades, y por tanto riesgos de auditoría. Dicho cuadro solo es un ejemplo de posibles situaciones conflictivas y, por tanto, debe adaptarse a la realidad en cada entidad. En la práctica debe analizarse como está estructurado el proceso de gestión en cada entidad fiscalizada, ya que las funciones principales y, en consecuencia, sus conflictos, dependen de cada caso específico. Por ejemplo, será diferente el proceso de compras de una entidad con sujeción plena a la LCSP al de una que no lo está.

El procedimiento de auditoría lógico consistiría en completar el formulario del Anexo 1 y, en cada subproceso, hacerse las pertinentes preguntas relacionadas con la gestión de compras y documentar las respuestas y la evidencia obtenida sobre los posibles conflictos de segregación de funciones y sus consecuencias en nuestra evaluación del control interno y valoración del riesgo.
Si no es adecuada la segregación de funciones se debe explicar por qué y hasta qué punto puede afectar al riesgo de auditoría. Se deben concretar los riesgos que puede provocar la falta de segregación. Se debe indagar si existen controles compensatorios que mitiguen los riesgos cuando no existe un control directo efectivo.

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

SF	Función 1	Función 2	Riesgo	F1 SAP	F2 SAP
1	Mantenimiento fichero maestro de proveedores	Aprobación pedidos / compras	Un usuario podría crear un proveedor ficticio o crear uno no autorizado y hacer una compra indebida.	XK01 Crear Proveedor (centralmente) FK01 Crear Proveedor (contablemente) MK01 Crear Proveedor (compras) FK02, MK02, XK02 , modificar proveed.	ME28 Liberar pedido de forma colectiva ME29N Liberar pedido individual
2	Mantenimiento fichero maestro de proveedores	Contabilización de facturas	Un usuario podría crear un proveedor ficticio o cambiar la cuenta de un proveedor existente y tramitar una factura ficticia.	XK01 Crear Proveedor (centralmente) FK01 Crear Proveedor (contablemente) MK01 Crear Proveedor (compras) FK02, MK02, XK02 , modificar proveed.	MIRO, Introducir factura FB60 Contabilizar factura FB65 Contabilizar abonos MRBR Liberar facturas bloqueadas (FB01,FB02, F26, F43, FB01, FB10, MR01, MRHR)
3	Mantenimiento fichero maestro de proveedores	Pagos	Un usuario podría crear un proveedor ficticio o cambiar la cuenta de un proveedor existente y dirigir a ella el pago de una factura existente.	XK01 Crear Proveedor (centralmente) FK01 Crear Proveedor (contablemente) MK01 Crear Proveedor (compras) FK02, MK02, XK02 , modificar proveed.	F-110 Pagos automáticos F-111 Pagos F-31 Pagos F-48 Anticipo F-53 Pagos
4	Creación del pedido de compra	Aprobación pedidos / compras	No debe permitirse crear y autorizar (liberar) el mismo documento de compra ya que podría producirse la aprobación indebida de documentos de compra.	ME21N Crear pedido ME22N Modificar pedido ME21 ME22	ME28 Liberar pedido de forma colectiva ME29N Liberar pedido individual
5	Aprobación pedido / compras	Recepción	Se puede aprobar una compra y realizar una recepción ficticia o apropiarse indebidamente de la misma.	ME28 Liberar pedido de forma colectiva ME29N Liberar pedido individual	MB1C Entrada mercancías MB11 Movimiento de mercancías MIGO Entrada de mercancías (MB01 Entrada de materiales Pedido de compra conocido MB0A Entrada de materiales Pedido de compra desconocido)
6	Aprobación pedido / compras	Pagos	Un usuario puede aprobar compras no autorizadas y realizar su pago sin mayor aprobación de la dirección.	ME28 Liberar pedido de forma colectiva ME29N Liberar pedido individual	F-110 Pagos automáticos F-111 Pagos F-31 Pagos F-48 Anticipo F-53 Pagos
7	Recepción de bienes	Contabilidad de facturas	Existiría el riesgo de que una persona procesara una factura y lo encubriera con una	MB1C Entrada mercancías MB11 Movimiento de mercancías MIGO Entrada de mercancías	MIRO, Introducir factura FB60 Contabilizar factura FB65 Contabilizar abonos

SF	Función 1	Función 2	Riesgo	F1 SAP	F2 SAP
			entrada de bienes incorrecta, lo que provocaría un pago indebido	(MB01 Entrada de materiales Pedido de compra conocido MB0A Entrada de materiales Pedido de compra desconocido)	(FB01,FB02, F26, F43, FB01, FB10, MR01, MRHR)
8	Contabilidad de facturas	Pagos	Un usuario puede crear facturas fraudulentas y procesar su pago automático.	MIRO, Introducir factura FB60 Contabilizar factura FB65 Contabilizar abonos (FB01,FB02, F26, F43, FB01, FB10, MR01, MRHR)	F-110 Pagos automáticos F-111 Pagos F-31 Pagos F-48 Anticipo F-53 Pagos
9	Pagos	Mantenimiento de bancos	Un usuario puede crear una cuenta ficticia y realizar pagos a la misma.	F-110 Pagos automáticos F-111 Pagos F-31 Pagos F-48 Anticipo F-53 Pagos	FI01,FI02,FI07, FI12
10	Aprobación pedido / compras	Introducción de facturas (contabilidad)	Un usuario puede crear un pedido ficticio e introducir una factura falseada.	ME28 Liberar pedido de forma colectiva ME29N Liberar pedido individual	MIRO, Introducir factura FB60 Contabilizar factura FB65 Contabilizar abonos (FB01,FB02, F26, F43, FB01, FB10, MR01, MRHR)
11	Mantenimiento del maestro de materiales/servicios	Recepción	Pagos indebidos debido a una petición de servicio y su posterior aceptación.	MM01, MM02 Modificar FMM	MB1C Entrada mercancias MB11 Movimiento de mercancias MIGO Entrada de mercancias (MB01 Entrada de materiales Pedido de compra conocido MB0A Entrada de materiales Pedido de compra desconocido)
12	Recepción	Mantenimiento del inventario	Un usuario podría registrar un activo, procesar una recepción de compras para registrar dicho activo y apropiarse indebidamente de él.	MB1C Entrada mercancias MB11 Movimiento de mercancias MIGO Entrada de mercancias (MB01 Entrada de materiales Pedido de compra conocido MB0A Entrada de materiales Pedido de compra desconocido)	AS01 Crear registro en FMaestro AS02 AS06
12	Mantenimiento fichero maestro de proveedores	Recepción	Apropiación indebida de materiales al introducir información incorrecta de recepción	XK01 Crear Proveedor (centralmente) FK01 Crear Proveedor (contablemente)	MB1C Entrada mercancias MB11 Movimiento de mercancias

SF	Función 1	Función 2	Riesgo	F1 SAP	F2 SAP
			de compras y modificar el maestro de proveedores.	MK01 Crear Proveedor (compras) FK02, MK02, XK02 FK05, MK05, XK05 FK06, MK06, XK06	MIGO Entrada de mercancias (MB01 Entrada de materiales Pedido de compra conocido MB0A Entrada de materiales Pedido de compra desconocido)
14	Mantenimiento fichero maestro de proveedores	Reconciliaciones bancarias	Un usuario podría cambiar la cuenta del proveedor y falsear las reconciliaciones bancarias para ocultar apuntes relacionados con ese proveedor.	XK01 Crear Proveedor (centralmente) FK01 Crear Proveedor (contablemente) MK01 Crear Proveedor (compras) FK02, MK02, XK02 FK05, MK05, XK05 FK06, MK06, XK06	FF67 Contabilización manual bancos FEBA_BANK_STATEMENT

En las dos primeras columnas del cuadro se señalan las funciones incompatibles, con carácter general. Las dos últimas columnas muestran las transacciones que activan dichas funciones en un sistema SAP con mayor frecuencia (siempre será necesario revisar la implantación/configuración de SAP en la entidad fiscalizada).

10. Identificación y revisión de las interfaces

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.

Estas interfaces, que sirven para transferir datos de una aplicación a otra, son un área significativa de riesgo para mantener la integridad de los datos económicos y la confidencialidad de la información.

Por ejemplo, una empresa utiliza una aplicación para gestionar las compras y relaciones con los proveedores 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.

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 mitigar esos riesgos.

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

Pueden identificarse deficiencias de control como las de los siguientes ejemplos:

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.

Además de revisar el adecuado diseño y funcionamiento operativo de los controles, se utilizarán en la mayor parte de los casos herramientas de análisis de datos, tipo ACL/IDEA, para comprobar el buen funcionamiento de las interfaces. La realización de pruebas masivas de datos permitirá en muchos casos comprobar el 100% de las transferencias de datos de una interfaz, cruzando la información de la aplicación de origen con la información de la aplicación de destino.

11. Revisión del cumplimiento legal

El objetivo del trabajo de fiscalización de la legalidad en el área de compras consiste en comprobar que se cumple la normativa aplicable en todas las etapas de su gestión. Normalmente esto es objeto de fiscalización en el área de contratación.

12. Procedimientos y programas 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 en los que se recogen dichos procedimientos 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.

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.
- Identificación de las aplicaciones informáticas de gestión significativas (las que soportan los procesos de gestión significativos) y de las principales interfaces.
- Documentar la comprensión del proceso de gestión.
- Dibujar un flujograma del proceso completo.
- Revisar las conclusiones de la revisión de los CGTI relacionados con el proceso de gestión auditado.
- Identificación de los riesgos inherentes en las afirmaciones y de los CPI.
- Realización de pruebas paso a paso y evaluación de la eficacia del diseño de los controles.
- Realización de pruebas del funcionamiento operativo de los controles.
- Procedimientos sustantivos.

Pruebas de datos

Normalmente la auditoría de los gastos de personal conlleva la realización de numerosas pruebas de datos, analizando la información existente en las bases de datos de personal y nóminas. En las pruebas de datos es aplicable la GPF-OCEX 5370.

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.

13. Colaboración de expertos en auditoría de sistemas de información

La realización de algunos de los procedimientos de auditoría descritos en esta guía requerirá la colaboración de expertos en auditoría de sistemas de información con el equipo de fiscalización encargado del trabajo. Con esa finalidad, el auditor responsable se pondrá en contacto con dichos expertos al iniciar la planificación del trabajo para coordinar la colaboración.

14. Aplicación de esta guía

Esta guía se aplicará en las auditorías de seguridad razonable en las que el área de compras de bienes y servicios sea un componente significativo de las cuentas anuales o cuando así se prevea en el programa de actuación o en la planificación de una fiscalización.

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.

Anexo 1: Documentar la comprensión del proceso de gestión de compras

El auditor debe describir y documentar su comprensión del proceso de gestión de compras, gastos y proveedores ejecutado por la Entidad.

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

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

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

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

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

##########

Entidad: _____

Fecha CCAA: _____

Resumen realizado por (Técnico/fecha): _____

Revisado por (Auditor/fecha): _____

1. Presupuestación

Este subproceso comprende el conjunto de actividades llevadas a cabo para calcular una estimación lo más precisa posible del presupuesto anual de gastos por compras, aprobación del presupuesto por el órgano que corresponda (Cortes, Pleno de un ayuntamiento,…) y su contabilización.

Describir:

a) Departamento/servicio que realiza esta función:

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

c) El proceso de previsión presupuestaria es autorizado de la siguiente forma:

d) La previsión presupuestaria se contabiliza de la siguiente forma:

(Señalar cuándo y cómo se contabilizan los AD's, todos al principio del año o mensualmente).

e) Persona responsable entrevistada:

f) Consideraciones sobre la segregación de funciones:

g) Indicar si existe un manual de procedimientos:

2. Mantenimiento del fichero maestro de proveedores (FMP)

a) Los cambios en el FMP se inician de la siguiente forma:

b) Los cambios en el FMP son autorizados de la siguiente forma:

c) Los cambios en el FMP son registrados de la siguiente forma:

d) Los cambios en el FMP son procesados de la siguiente forma:

e) Los cambios en el FMP son reconciliados con la información del proveedor de la siguiente forma:

f) Persona responsable entrevistada

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

- *Hemos revisado los procedimientos de la entidad archivados en el AP.*
- *Nos hemos entrevistado el __/__/2023 con la persona responsable.*
- *Hemos realizado una prueba de recorrido archivada en (Ref).*
- *Hemos realizado un flujograma archivado en (Ref).*
- *Otros procedimientos.*

3. Gestión de las compras

Esta fase del proceso se encuentra directamente afectada por la forma en que la entidad haya implantado la normativa de la LCSP, por tanto, debe tenerse muy presente, en su caso, lo establecido en las Instrucciones de contratación de la entidad.

a) Los pedidos se inician de la siguiente forma:

b) Los pedidos son autorizados de la siguiente forma:

c) Los pedidos son registrados de la siguiente forma:

d) Los pedidos son procesados de la siguiente forma:

e) Los registros de pedidos son reconciliados con la información de los bienes y servicios recibidos de la siguiente forma:

f) Persona responsable entrevistada

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

4. Recepción de bienes y servicios

a) A la recepción de bienes se inician las siguientes acciones:

b) La recepción de bienes es autorizada de la siguiente forma:

c) La recepción de bienes es registrada de la siguiente forma:

d) La recepción de bienes es procesada y contabilizada de la siguiente forma:

e) Los listados (registros) de bienes recibidos son reconciliados con los listados de inventario y/o con el auxiliar de proveedores y saldos de las cuentas de mayor de la siguiente forma:

f) Persona responsable entrevistada

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

5. Devoluciones

a) La devolución de bienes se inicia de la siguiente forma:

b) Las devoluciones de bienes son autorizadas de la siguiente forma:

c) Las devoluciones de bienes son registradas de la siguiente forma:

d) Las devoluciones de bienes son procesadas y contabilizadas de la siguiente forma:

e) Las devoluciones de bienes son reconciliadas con los listados de inventario y/o con el auxiliar de proveedores y saldos de las cuentas de mayor de la siguiente forma:

f) Persona responsable entrevistada

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

6. Tramitación de las facturas

a) Las transacciones en las cuentas de proveedores se inician de la siguiente forma:

b) Las transacciones en las cuentas de proveedores son autorizadas de la siguiente forma:

c) Las transacciones en las cuentas de proveedores son registradas de la siguiente forma:

d) Las transacciones en las cuentas de proveedores son procesadas y contabilizadas de la siguiente forma:

e) Las transacciones en las cuentas de proveedores son reconciliadas con el auxiliar de proveedores y saldos de las cuentas de mayor de la siguiente forma:

f) Persona responsable entrevistada

Los procedimientos que hemos realizado para verificar nuestra comprensión (tal como está descrita) de la tramitación de las facturas han sido los siguientes:

7. Pagos

a) El proceso de pago se inicia de la siguiente forma:

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

c) Los pagos son registrados de la siguiente forma:

d) El proceso de pagos es procesado de la siguiente forma:

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

f) Persona responsable entrevistada

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

8. Soporte informático

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

Gestión de compras: SAP/Microsoft Dynamics/Desarrollo propio/Otra
Gestión de proveedores:
Gestión de tesorería:
Contabilidad:

9. Flujograma general (resumido)

Poner o referenciar.

10. Conclusión

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

- *Hemos revisado los procedimientos de la entidad archivados en el AP.*
- *Nos hemos entrevistado el __/__/20xx con la persona responsable.*
- *Hemos realizado una prueba paso a paso archivada en (Ref.).*
- *Hemos realizado un flujograma archivado en (Ref.).*
- *Otros procedimientos.*

Los controles previstos en los procedimientos de gestión de compras de la entidad, si son efectivos, permitirán que los procedimientos sustantivos planificados puedan proporcionar evidencia de auditoría suficiente y adecuada para poder concluir sobre la razonabilidad de las cifras de gastos por compras de bienes y servicios.

O bien:

Los controles previstos en los procedimientos de gestión de compras de la entidad no garantizan que los procedimientos sustantivos, por sí solos, puedan proporcionar evidencia de auditoría suficiente y adecuada para poder concluir sobre la razonabilidad de las cifras de gastos de compras de bienes y servicios, ya que ….*(señalar las afirmaciones y aquellos aspectos que se considera deben ser analizados valorando el sistema de control interno y su fiabilidad).*