Guía práctica de fiscalización de los OCEX

GPF-OCEX 5340: Los controles de aplicación: qué son y cómo revisarlos

Referencia: ISSAI 5300, GPF-OCEX 5300 y GPF-OCEX 1315

Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de ASOCEX el 12/11/2018

1. Introducción

El enfoque de auditoría basado en el análisis del riesgo es el fundamento central de la actividad auditora desarrollada bajo las Normas Internacionales de Auditoría (NIA-ES) y las ISSAI-ES. Tal como señala la GPF-OCEX 1315, "de acuerdo con este enfoque, el objetivo del auditor es obtener una seguridad razonable de que las cuentas anuales en su conjunto están libres de incorrecciones materiales, debidas a fraude o error. Una seguridad razonable es un grado alto de seguridad y se alcanza cuando el auditor ha obtenido evidencia de auditoría suficiente y adecuada para reducir el riesgo de auditoría (es decir, el riesgo de expresar una opinión inadecuada cuando las cuentas anuales contengan incorrecciones materiales) a un nivel aceptablemente bajo. No obstante, una seguridad razonable no significa un grado absoluto de seguridad, debido a que existen limitaciones inherentes a la auditoría que hacen que la mayor parte de la evidencia de auditoría a partir de la cual el auditor alcanza sus conclusiones y en la que basa su opinión sea más convincente que concluyente."

Actualmente, en una auditoría financiera basada en el análisis de los riesgos realizada de acuerdo con la ISSAI-ES 200, el estudio y revisión de los sistemas de información en los que se sustenta la gestión de una entidad (empresa o fundación pública, ayuntamiento, administración de la comunidad autónoma, etc.) se ha convertido en una actividad de importancia creciente, en la medida en que esa gestión se apoya en unos sistemas de información interconectados que, con la plena implantación de la administración electrónica, han ido adquiriendo una complejidad cada vez mayor. Esta situación ha generado una serie de nuevos e importantes riesgos de auditoría (inherentes y de control) que deben ser considerados en la estrategia de auditoría.

Para orientar y facilitar a los auditores de los OCEX la aplicación del enfoque de riesgo y la auditoría en entornos de administración electrónica se han desarrollado las Guías Prácticas de Fiscalización (GPF-OCEX).

De acuerdo con las ISSAI-ES/NIA-ES, dentro del proceso auditor, la revisión de los controles internos implementados en las aplicaciones informáticas de gestión y en las interfaces es un aspecto muy relevante, tanto más importante cuanto más complejo sea el sistema de información que soporta el proceso de gestión incluido en el alcance de la auditoría.

En el Anexo 2 de la GPF-OCEX 1315 se detallan los pasos a seguir para analizar un sistema de información e identificar los procesos, las aplicaciones de gestión significativas, y las interfaces de interés para la auditoría. El conocimiento de estos elementos es una parte esencial de la planificación de una auditoría.

Desde el punto de vista metodológico/cronológico la revisión de los controles de aplicación se hará siempre tras la revisión de los controles generales de tecnologías de la información (véase la GPF-OCEX 5330), respecto de los que existe una elevada dependencia, tal como se comentará más adelante.

Muy esquemáticamente, según la citada GPF-OCEX 1315, las etapas de una auditoría ejecutada con el enfoque basado en el análisis de los riesgos son las mostradas en la Figura 1.

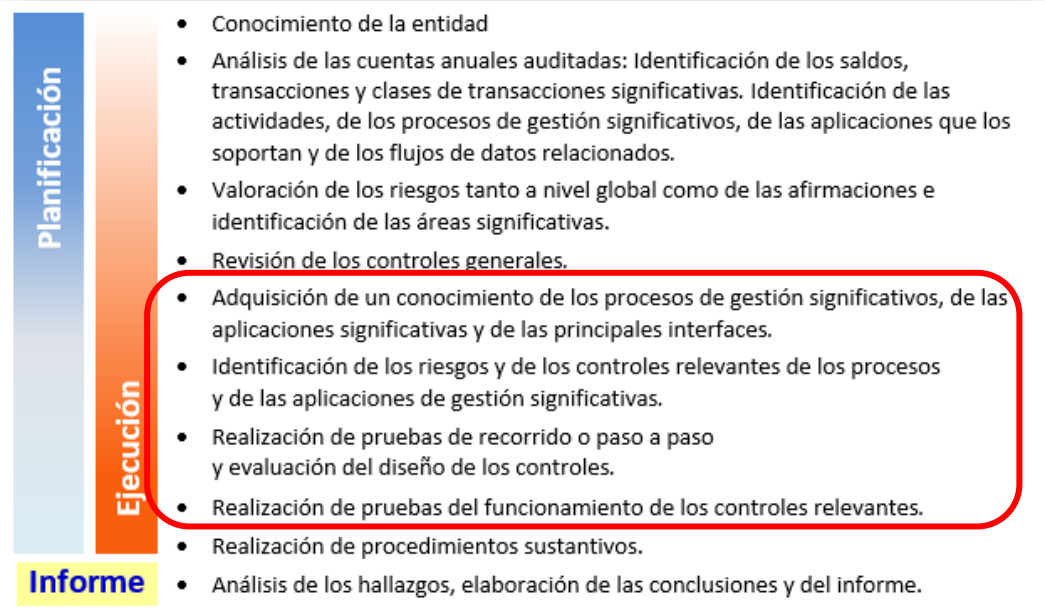


Figura 1

En el Anexo 4 de la GPF-OCEX 1315 se incluye un flujograma típico de una auditoría.

2. Objetivos de esta etapa de la auditoría

En este documento vamos a centrarnos en el estudio de la etapa de revisión de los controles de aplicación y de los controles sobre las interfaces, cuya finalidad es:

- Adquirir un conocimiento profundo de los procesos de gestión revisados, de los riesgos significativos existentes en las aplicaciones informáticas que los soportan y en las interfaces relacionadas.
- Identificar, analizar y comprobar el adecuado funcionamiento de los controles de los procesos y aplicaciones de gestión y de los controles sobre las interfaces.
- Determinar la extensión de los procedimientos sustantivos a ejecutar.
- Reducir el riesgo de auditoría a un nivel aceptable.

El **objetivo de la auditoria de los controles de aplicación** será obtener una seguridad razonable de que el sistema de control interno garantiza la integridad (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 controles relevantes garantiza la correcta ejecución de los procesos de gestión auditados y mitigan el riesgo de errores e irregularidades.

3. Los controles internos

3.1 En la GPF-OCEX 1315 se define el control interno como el proceso diseñado, implementado y mantenido por los responsables del gobierno de la entidad, la dirección y otro personal, con la finalidad de proporcionar una seguridad razonable sobre la consecución de los objetivos de la entidad relativos a la fiabilidad de la información financiera, la eficacia y eficiencia de las operaciones, así como sobre el cumplimiento de las disposiciones legales y reglamentarias aplicables.

Un control es la combinación de métodos, políticas y procedimientos que garantizan la protección de los activos de la organización, la precisión y la confiabilidad de sus registros, y el cumplimiento las directrices de la dirección en la consecución de dichos objetivos.

Las actividades de control o controles internos pueden estar totalmente automatizadas (circunstancia habitual en los actuales sistemas informáticos de gestión), pueden ser manuales dependientes de las TIC (bastante frecuentes también) o completamente manuales (cada vez más escasos).

En una auditoría financiera se considerará que un sistema de control interno es efectivo si los controles son respetados y dan una seguridad razonable de que no habrá errores o irregularidades que afecten de manera significativa a los estados financieros.

3.2 ¿Por qué los controles de TI son importantes para el auditor de sistemas de información?[1]

Generalmente, el auditor de TI es solicitado para evaluar los controles relacionados con la tecnología, mientras que los auditores que no auditan las TI evalúan los controles financieros, regulatorios y de cumplimiento. A medida que cada vez más organizaciones dependen de TI para automatizar sus operaciones, la línea que divide la función de los auditores de TI y los auditores que no auditan las TI se reduce rápidamente. Como mínimo, se requiere que todos los auditores comprendan el entorno de control de la entidad auditada con el fin de brindar seguridad respecto de los controles internos que operan en la entidad. De conformidad con los Principios Fundamentales de Auditoría del Sector Público de ISSAI: "Los auditores deben comprender la naturaleza de la entidad/programa a ser auditado". Esto incluye la comprensión de los controles internos, los objetivos, las operaciones, el entorno regulatorio y los sistemas y procesos del negocio involucrados.

Cada área de control se basa en un conjunto de objetivos de control que una organización implementa a fin de mitigar riesgos. La función del auditor es entender los riesgos potenciales del negocio y de TI que enfrenta la entidad auditada y, a su vez, evaluar si los controles implementados son los adecuados para cumplir con los objetivos de control.

3.3 Debemos hacer una primera distinción muy importante entre[2]:

- Los **controles generales de las tecnologías de la información (CGTI).** Afectan a todos los niveles de los sistemas de información, si bien están relacionados con mucha mayor intensidad con aquellos niveles de carácter general que afectan a toda la organización y a los sistemas TI. Son políticas y procedimientos vinculados a muchas aplicaciones y favorecen un funcionamiento eficaz de los controles de las aplicaciones. Son analizados en la GPF-OCEX 5330.
- Los **controles de aplicación.** Operan al nivel de los procesos de gestión y que se aplican al procesamiento de las transacciones mediante aplicaciones informáticas específicas.

3.4 A los efectos de esta guía, podemos representar el sistema de información de una entidad mediante un modelo simplificado formado por cinco niveles o capas tecnológicas superpuestas, tal como se muestra en la figura 2.

[1] Manual sobre auditoría TI para las Entidades Fiscalizadoras Superiores de INTOSAI.
[2] Véase GPF-OCEX 1316; apartado 9.2.

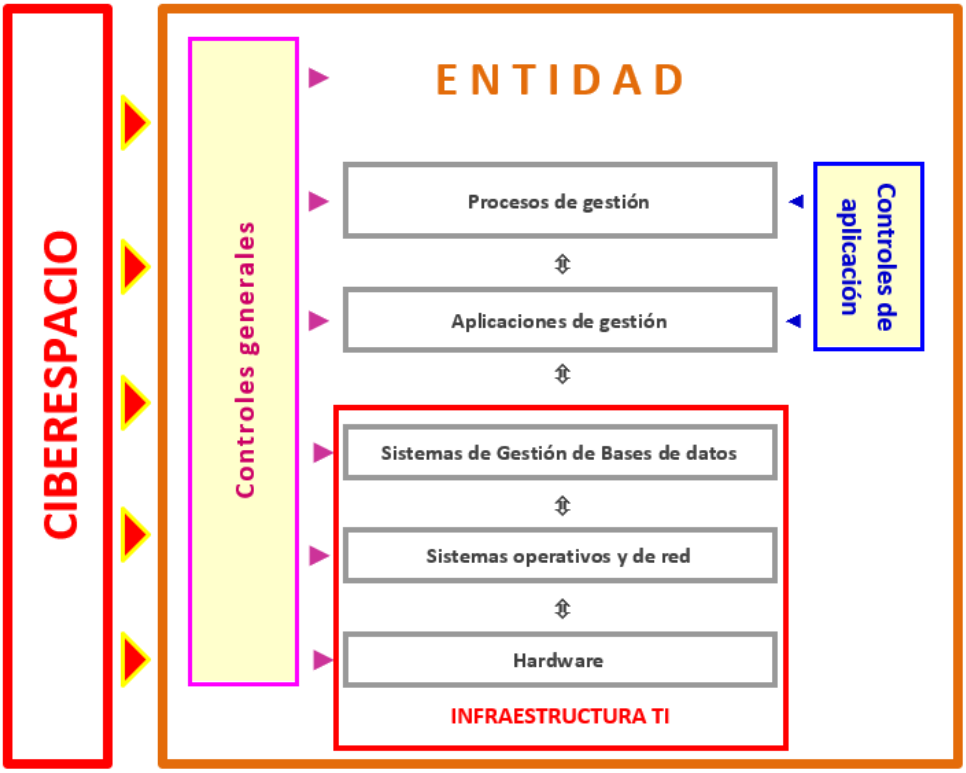


Figura 2

3.5 Además, los controles se clasifican en tres tipos:

Tipo	Características	Ejemplos
Preventivo	Su finalidad es prevenir que ocurra un hecho que no es consistente con los objetivos de control. Detecta los problemas antes de que sucedan. Monitoriza las operaciones y los inputs y previene errores, omisiones o actos malintencionados.	• Separar las funciones de aprobación de un gasto y de su pago. Este control está diseñado para reducir el riesgo de pagos indebidos. • Limitar el acceso a los sistemas TIC. Limitar el acceso mediante roles y passwords a cambiar programas reduce el riesgo de transacciones no autorizadas.
Detectivo	Detectan e informan de la ocurrencia de un error, omisión o acto malintencionado.	• Conciliaciones. Comparar por persona independiente dos conjuntos de datos relativos a la misma transacción y analizar las diferencias permite detectar errores o irregularidades.
Compensatorio	Si es efectivo, puede limitar o mitigar la gravedad de una deficiencia de control interno. Limitan la gravedad de una deficiencia y sus consecuencias, pero no la eliminan.	• En entidades de reducida dimensión los controles de segregación de funciones pueden ser difíciles de implantar y deben compensarse con controles que impliquen una mayor supervisión o control gerencial.

Figura 3

4. Concepto de control de aplicación

4.1 Los controles de aplicación 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 aplicación informática.**

Ejemplos de controles de aplicación incluyen la comprobación de la exactitud aritmética de los registros, el mantenimiento y revisión de las cuentas y balances de comprobación, controles automatizados tales como filtros de datos de entrada y comprobaciones de secuencia numérica, y el seguimiento manual de los informes de excepciones.

4.2 La **finalidad de los controles de aplicación** en un entorno informatizado es establecer procedimientos de control específicos sobre las aplicaciones de gestión con el fin de asegurar razonablemente que todas las transacciones son autorizadas y registradas, y que son procesadas de forma completa, adecuada y oportuna, y de garantizar la exactitud de los resultados. En consecuencia, los controles juegan un papel central en la realización de los objetivos de la entidad, de la protección del patrimonio, de la exactitud y de la fiabilidad de la contabilidad y del respeto a las normas.

Actualmente los procesos de gestión de los entes públicos están automatizados en buena medida y la tendencia es que con la implantación de la administración electrónica los controles internos estén 100% automatizados o sean TI dependientes; los controles 100% manuales tienden a desaparecer. No obstante, cuando se revisa un proceso de gestión (nóminas, compras, recaudación, etc.) se analiza en su integridad, identificando todos los riesgos significativos y los controles relevantes, independientemente de si el proceso o los controles están automatizados o son manuales. Todos los controles internos relevantes del proceso de gestión deben auditarse, sean manuales o automáticos.

4.3 Desde el punto de vista del auditor, los **objetivos generales** de los controles de las aplicaciones / procesos de gestión son proporcionar una seguridad razonable de que las transacciones y los datos son **completos, exactos, válidos y de que se ha cumplido con la legalidad** en la gestión de las transacciones.

Estos objetivos pueden describirse así[3]:

- Los controles de **integridad**[4] (entendida como **completitud**) proporcionan una seguridad razonable de que:
  - todas las transacciones reales son introducidas en el sistema,
  - si son válidas son aceptadas en el procesamiento,
  - son procesadas una sola vez, los duplicados son rechazados,
  - las transacciones rechazadas son identificadas, corregidas y reprocesadas; y
  - todas las transacciones aceptadas por el sistema son procesadas completamente.

  Los controles más usuales son: totales de lotes, control de secuencia, control de duplicados, reconciliaciones, totalizadores e informes de excepción.

- Los controles de **exactitud** proporcionan una seguridad razonable de que:

[3] Véase FISCAM 2009, GAO, apartado 4.0.1.

[4] En español se traduce de la misma forma, como integridad, dos términos *integrity* y *completeness* que tienen un significado distinto en el original en inglés de las normas de auditoría, lo que provoca una cierta confusión de conceptos.

Integridad *(integrity)* es la garantía de que los datos o información de origen han sido validados y estos no han sido alterados al ser creados, procesados, transmitidos y almacenados en los sistemas informáticos (GPF-OCEX 1500, apartado 37).

De forma similar, según el ENS la integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales

Debe distinguirse de integridad en el sentido de completitud (*completeness*). En este documento cuando se utilice integridad en este sentido se indicará así: *integridad (completitud)*.

- las transacciones son registradas adecuadamente, con la fecha e importes correctos, en tiempo oportuno y en el periodo adecuado;
- los datos son procesados de forma exacta por las aplicaciones, que producen resultados fiables con output exactos.

Se incluyen: validaciones, comprobaciones automáticas de razonabilidad, de dependencia, de existencia, de formato, de rangos, de exactitud matemática, etc.

- Los controles de **validez** proporcionan una seguridad razonable de que:
  - todas las transacciones registradas han ocurrido realmente, corresponden a la Entidad y han sido adecuadamente aprobadas; y de que
  - el output contiene solo datos válidos.

  Una transacción es válida cuando ha sido debidamente autorizada y cuando los datos maestros relativos a esa transacción son **fiables** (por ejemplo los datos bancarios o domicilio del acreedor). La validez incluye el concepto de **autenticidad**.

  Ejemplo: comprobar una factura con el pedido y el albarán de entrada antes de su aprobación..

- Los controles de **legalidad** proporcionan una seguridad razonable de que en la gestión de las operaciones se ha cumplido con la legalidad vigente.

Estas características coinciden con las afirmaciones implícitas en la información financiera según la GPF-OCEX 1317.

Adicionalmente, los controles de **integridad**, de **confidencialidad** y de **disponibilidad** los consideramos CGTI al nivel del proceso o aplicación:

- Los controles de **integridad** proporcionan una seguridad razonable de que la información procesada o almacenada no puede ser alterada o manipulada por personas no autorizadas.
- Los controles de **confidencialidad** proporcionan una seguridad razonable de que los datos, informes y otros outputs son protegidos contra accesos no autorizados.
- Los controles de **disponibilidad** proporcionan una seguridad razonable de los datos e informes de la aplicación están accesibles a los usuarios cuando se necesitan.

Estos, principalmente son controles relacionados con la seguridad de la información, las copias de seguridad y la planificación de las contingencias, y en consecuencia no se consideran específicamente controles de procesos de gestión, sino CGTI al nivel de la aplicación.

4.4 Por otra parte, cada control interno o actividad de control tendrá sus **objetivos específicos de control**. Para más detalle ver el Anexo 3.

4.5 Cada tipo de aplicación exige controles diferentes, ya que cada proceso de gestión o actividad comercial, industrial, o de servicio específica, comporta riesgos diferentes, inherentes a esa actividad y susceptibles de perjudicar o impedir alcanzar los objetivos. Por ello, cada actividad de control está diseñada específicamente para alcanzar uno o varios de estos objetivos. La eficacia de los controles de aplicación depende de si todos estos objetivos generales han sido alcanzados.

5. Interrelación de los CGTI con los controles de aplicación

5.1 Los CGTI ayudan a asegurar el correcto funcionamiento de los sistemas de información mediante la creación de un entorno adecuado para el correcto funcionamiento de los controles de aplicación. Sin unos controles generales efectivos, los controles de aplicación pueden dejar de ser efectivos ya que resultará mucho más fácil eludirlos.

Una evaluación favorable de los CGTI da confianza al auditor sobre los controles de aplicación automatizados integrados en las aplicaciones de gestión.

Por ejemplo, la emisión y revisión manual de un informe especial de elementos no coincidentes puede ser un control de aplicación efectivo; no obstante, dicho control dejará de ser efectivo si los controles generales permitiesen realizar modificaciones no autorizadas de los programas, de forma que determinados elementos quedasen excluidos deliberadamente de manera indebida del informe revisado.

Unos CGTI ineficaces pueden impedir que los controles de aplicación funcionen correctamente y permitir que se den manifestaciones erróneas significativas en las cuentas anuales y que éstas no sean detectadas. Por tanto, **la importancia de una deficiencia de un CGTI debe ser evaluada en lo que se refiere a su efecto en los controles de aplicación**, es decir, comprobar si los controles de aplicación dependientes son ineficientes.

Por ejemplo, garantizar la seguridad de las bases de datos se considera un requisito indispensable para que la información financiera sea fiable. Sin seguridad a nivel de base de datos, las entidades estarían expuestas a cambios no autorizados en la información financiera.

5.2 La NIA-ES 330 establece que al diseñar y ejecutar pruebas de controles el auditor determinará si los controles a comprobar dependen a su vez de otros controles (controles indirectos) y, si es así, si es necesario obtener evidencia adicional de auditoría que acredite el funcionamiento efectivo de dichos controles indirectos.

Por ejemplo: un control consistente en la revisión manual de un informe de excepción sobre ventas que hayan excedido los límites de crédito autorizados. La revisión del responsable y el consiguiente seguimiento es el control relevante para el auditor. Los controles sobre la precisión de la información incluida en los informes (por ejemplo, los controles generales) se denominan controles indirectos y también hay que asegurarse que están incluidos en el alcance.

Otro ejemplo: una entidad puede tener correctamente configurada la segregación de funciones en el proceso de compras, contabilidad y pago; pero si no existe un CGTI que establezca mecanismos de identificación y autenticación de los usuarios que sea eficaz, todo el sistema de segregación de funciones devendrá a su vez en ineficaz.

Si no existieran controles generales o no fueran efectivos, no se podría confiar en los controles de aplicación y sería necesario adoptar un enfoque de auditoría basado exclusivamente en procedimientos sustantivos.

5.3 El reto con los CGTI consiste en que estos casi nunca afectan a la información financiera directamente, pero tienen un efecto generalizado y permanente en todos los controles internos. Es decir, si un CGTI importante falla (p. ej. un control de restricción de acceso a programas y datos), tiene un efecto dominante en todos los sistemas que dependen de él, incluidas las aplicaciones financieras; *por ejemplo, sin estar seguros de que solamente los usuarios autorizados tienen acceso a las aplicaciones financieras o a las bases de datos subyacentes, no se puede concluir que únicamente aquellos usuarios con autorización iniciaron y aprobaron transacciones.*

De una forma visual, vemos que unos controles generales débiles no protegen ni posibilitan de forma eficaz el buen funcionamiento de los controles de las aplicaciones:

Figura 4

Sin embargo, unos controles generales sólidos y eficaces, proporcionan un entorno adecuado para el buen funcionamiento de los controles de las aplicaciones:

Figura 5

Otro ejemplo: los controles de una aplicación de ventas-facturación pueden estar bien diseñados y correctamente implementados, pero si no hay controles sobre los accesos directos a las bases de datos que soportan y registran los datos y transacciones de la aplicación, aquellos controles son inútiles.

5.4 Por las razones señaladas al auditar el control interno de un proceso/aplicación de gestión es necesario revisar los controles existentes en toda la "pila" del sistema de información, es decir los controles de aplicación y los CGTI de todos los niveles del sistema de información que soportan el proceso de gestión auditado que afectan a su buen funcionamiento, tal como se muestra gráficamente en la Figura 6.

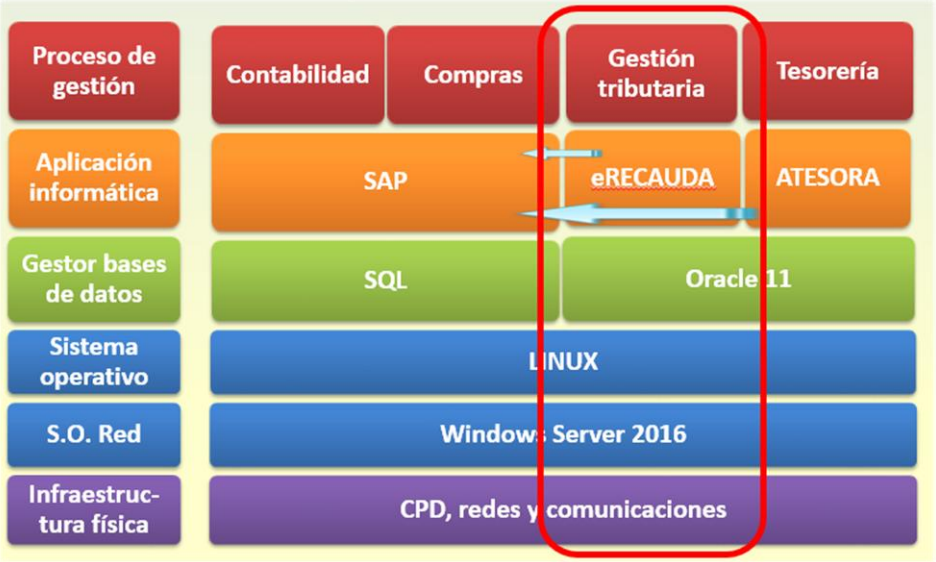


Figura 6

6. Adquisición de un conocimiento de los procesos de gestión significativos, de las aplicaciones significativas y de las principales interfaces.

Estas son unas de las primeras actividades que deben realizarse en una auditoría financiera realizada con el enfoque basado en el análisis del riesgo, tal como puede verse en la Figura 1. En la GPF-OCEX 1315 se explica la metodología general de auditoría de esa fase.

En los anexos 1 y 2 se dan unas orientaciones sobre cómo realizar y documentar este trabajo, que se debe plasmar en un flujograma detallado como el del ejemplo de gestión de ingresos tributarios de un ayuntamiento mostrado en la Figura 7, complementado con una narrativa explicativa.

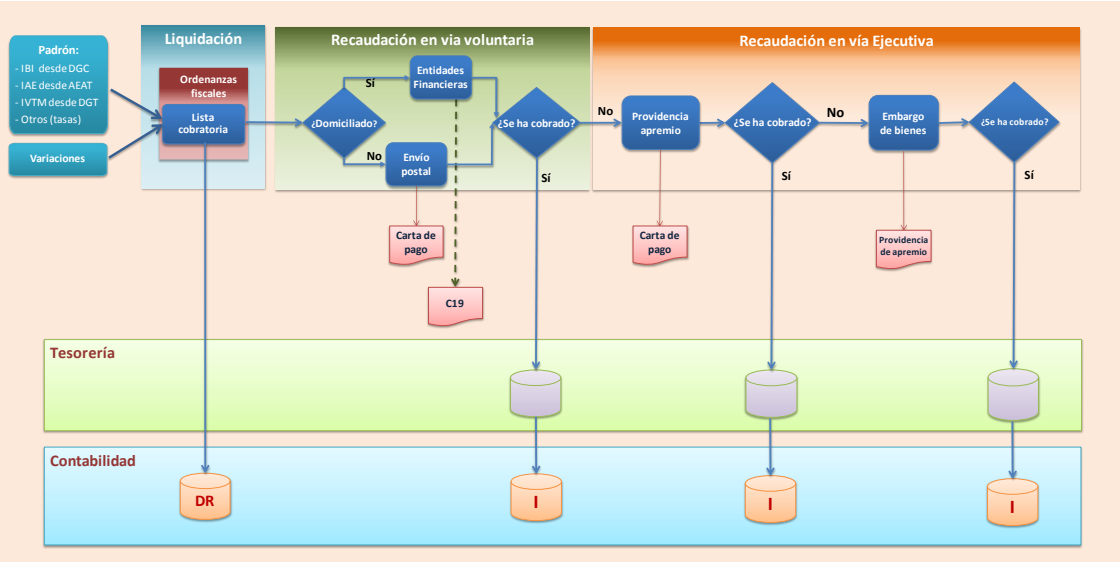


Figura 7

7. Identificación de los riesgos y de los controles relevantes de los procesos y aplicaciones de gestión significativas, y de las interfaces.

7.1 Una vez identificados los procesos y las aplicaciones de gestión que tienen carácter significativo en relación con las cuentas anuales, que son las incluidas dentro del alcance de la auditoría, y hecha la revisión de los controles generales con resultado satisfactorio (es decir se ha llegado a la conclusión de que son confiables), se pasa a la siguiente etapa de la auditoría.

Si tras la revisión de los CGTI se llegara a la conclusión de que no son eficaces, un auditor financiero deberá replantearse su estrategia de auditoría ya que no podrá confiar en los controles de aplicación y deberá adoptar un enfoque basado en pruebas sustantivas para realizar la auditoría financiera[5].

En esta etapa, el auditor TI se debe delimitar el alcance detallado de la auditoría a realizar sobre las aplicaciones de gestión seleccionadas. Teniendo en cuenta la complejidad de los procesos y de las aplicaciones de gestión en los actuales entornos de administración electrónica, es importante centrarse

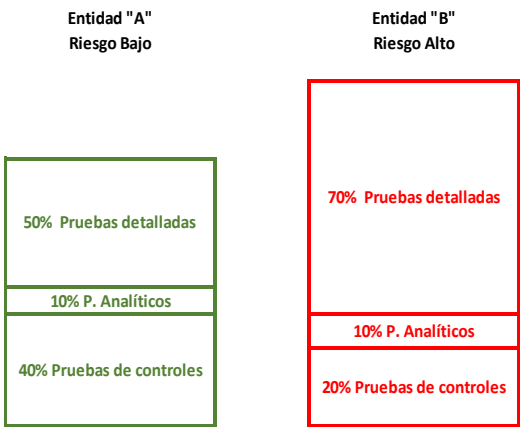
[5] La naturaleza, momento y alcance de los procedimientos de auditoría se determinan de acuerdo con las circunstancias de cada trabajo y deben basarse en el conocimiento de la actividad que realiza el ente auditado, de su organización, de los riesgos valorados así como en la evaluación del control interno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

Los procedimientos de auditoría financiera 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 y los tipos de pruebas necesarias para obtenerla



en lo esencial, por ello la identificación de los riesgos significativos y de los controles relevantes implantados para mitigarlos constituye la base para una auditoría eficaz. Solo se evaluará la efectividad de aquellos controles que tengan relevancia a efectos de la auditoría financiera, circunstancia que deberá ser definida por el auditor financiero con la colaboración del auditor de sistemas a partir de los riesgos significativos identificados.

Se deben identificar los riesgos existentes en los principales procesos de gestión y en los sistemas y aplicaciones que las soportan, lo que dará una idea general de los riesgos susceptibles de impedir la consecución de los objetivos del proceso de gestión o que puedan entrañar incorrecciones materiales en las cuentas anuales. Este análisis de los riesgos ayuda a definir la estrategia de auditoría, es decir de la confianza preliminar en la eficacia del control interno y del peso relativo de las pruebas de cumplimiento y de los procedimientos sustantivos.

Se partirá del estudio realizado del proceso/aplicación a auditar (ver apartado 6 anterior) y de cualquier otra documentación o información disponible del proceso/aplicación, incluyendo entrevistas con los usuarios o responsables de la entidad

Normalmente, al realizar el estudio y descripción de un proceso mediante una narrativa y un flujograma, se incluye una "primera versión" de los riesgos y controles clave identificados, que serán confirmados o modificados después al realizar las pruebas de recorrido.

7.2 La identificación de los riesgos potenciales se realiza consultando a los distintos usuarios o responsables del proceso de gestión auditado y analizando los distintos pasos y componentes que intervienen en el proceso:

- El flujo de procesamiento de los datos (ver Anexo 1)
- Los datos maestros (ver Anexo 3)
- Los permisos o autorizaciones (ver Anexo 1)
- La segregación de funciones (ver Anexo 4)
- Las interfaces (datos entrantes y salientes) (ver Anexo 2)

Además de identificar los riesgos inherentes del proceso de gestión (manual o automatizado) en su integridad, en las interfaces, en los parámetros y en los datos maestros, debe adquirirse una comprensión preliminar de los controles de aplicación que mitiguen dichos riesgos.

Todos los controles importantes ligados a las aplicaciones, que tengan una influencia directa sobre el resultado del proceso, deben ser tenidos en cuenta, **tanto los manuales como los automáticos**.

Normalmente existe una combinación de controles automatizados y manuales que equilibran los recursos materiales y humanos requeridos por el equipo auditor y la reducción del riesgo de auditoría.

7.3 Los **controles relevantes** son un elemento fundamental en la auditoría basada en el análisis del riesgo, ya que buena parte de los procedimientos de auditoría giran a su alrededor.

En esta fase, de todos los controles identificados en las aplicaciones revisadas, solo interesan los más importantes, los que, si están bien diseñados e implantados y funcionan con eficacia, permiten concluir al auditor que los riesgos de auditoría de que existan errores o irregularidades no detectados por el sistema de control interno están controlados en un nivel aceptable.

Es decir, **el auditor obtendrá conocimiento de las actividades de control relevantes para la auditoría** que, a juicio del auditor, son[6]:

- Aquellas que es necesario conocer, al ser actividades de control relacionadas con riesgos significativos.
- Aquellas que están relacionadas con riesgos para los cuales aplicar solo procedimientos sustantivos no proporciona evidencia de auditoría suficiente y adecuada.
- Las que, a juicio del auditor, de funcionar adecuadamente, permiten mitigar el riesgo de incorrección material (RIM) y reducir el riesgo de auditoría.

[6] Véase GPF-OCEX 1316; apartado 9.1.

El auditor debe poner énfasis en la identificación y la obtención de conocimiento de las actividades de control en aquellas áreas en las que considera más probable que existan riesgos de incorrección material.

7.4 Una auditoría no requiere el conocimiento de todas las actividades de control relacionadas con cada tipo significativo de transacción, de saldo contable y de información a revelar en los estados financieros o con cada afirmación correspondiente a ellos. Cuando múltiples actividades de control alcancen individualmente el mismo objetivo, no es necesario obtener conocimiento de cada una de las actividades de control relacionadas con dicho objetivo, bastará con verificar que uno de esos controles es eficaz.

7.5 A la hora de decidir si un control es relevante, debe aplicarse el juicio profesional, y se tendrá en cuenta lo siguiente:

- Los controles relevantes generalmente incluyen políticas, procedimientos, prácticas y una estructura organizativa que son esenciales para que la dirección pueda reducir los riesgos significativos y alcanzar el objetivo de control relacionado.
- Los controles relevantes a menudo respaldan más de un objetivo de control.
- Los controles que hacen frente directamente a los riesgos significativos son con frecuencia relevantes.
- Los controles preventivos son por regla general más eficientes que los detectivos. Por lo tanto, los controles preventivos se consideran a menudo relevantes.
- Los controles automatizados son más fiables que los controles manuales.

7.6 Para cada control que se haya identificado como relevante, el auditor debe aplicar **procedimientos** para **analizar la efectividad de su diseño para realizar la actividad de control**, considerando el riesgo TI y los objetivos de la auditoría. Si se concluye que el diseño es eficaz se aplicarán procedimientos de auditoría para **verificar si está implementado y en funcionamiento durante todo el periodo auditado**.

7.7 **Los controles relevantes** (a veces denominados controles clave)**, individualmente o combinados entre ellos, son indispensables para la reducción de los riesgos a un nivel aceptable**. Son los que permiten reducir los riesgos de incorrección material (RIM) a un nivel aceptablemente bajo.

Constituyen el elemento fundamental del sistema de control y deben ser, pues, objeto de comprobación prioritaria; los otros controles tienen menos importancia para el auditor. Si el auditor no se concentra sobre los controles relevantes, la auditoría corre el riesgo de ser demasiado general e ineficaz.

7.8 Todo el trabajo de auditoría posterior debe centrarse en los controles relevantes, ya que todo trabajo que se realice sobre los otros controles existentes no aporta satisfacción o utilidad adicional de auditoría, y será un trabajo ineficiente.

Ver consideraciones adicionales sobre los controles relevantes en el apartado 6 de la GPF-OCEX 5330.

8. Evaluación del diseño de los controles. Realización de pruebas de recorrido o paso a paso.

8.1 Tras la identificación de los controles relevantes que mitigan riesgos significativos (RIM si se está haciendo una auditoría financiera) el siguiente paso será evaluar el diseño de los controles para ver si son eficaces, es decir, para determinar si cada uno de estos controles, individualmente o en combinación con otros controles, es capaz de prevenir, detectar y corregir de forma efectiva errores o irregularidades materiales.

Si están bien diseñados se deberá verificar que han funcionado como se esperaba, que han estado operativos, durante todo el periodo auditado.

Solo una comprensión profunda del diseño de los controles permite definir una estrategia adecuada para la evaluación del funcionamiento de los controles mediante el diseño y ejecución de pruebas de cumplimiento que sean eficaces, plenamente adaptadas a la actividad de control.

8.2 El diseño de los controles, especialmente su situación en el proceso de gestión debe ser evaluado para saber si:

- Los riesgos identificados son cubiertos completamente.
- Los objetivos de control definidos pueden ser realmente alcanzados por los controles implantados.

- Los controles permiten realmente reducir los riesgos de errores y de irregularidades.
- La cobertura de los riesgos se realiza de forma eficaz y económica (eficiencia).
- Otro control o combinación de controles son más eficaces para realizar el mismo objetivo de control.

Un análisis minucioso del diseño de los controles permite:

- Identificar las lagunas, los solapamientos y los duplicados en materia de controles.
- Evitar realizar pruebas de controles por el auditor cuando los controles son inadecuados o ineficaces.
- Considerar si el mismo resultado o uno mejor, puede ser obtenido con la utilización o adaptación de otros controles, especialmente con otros ya establecidos.

La evidencia probatoria de la eficacia de los controles durante todo el periodo revisado solo puede ser obtenida mediante la realización de pruebas de controles.

8.3 Al evaluar el diseño de los controles deben considerarse los aspectos siguientes:

- ¿Las etapas del proceso y los controles relacionados están organizados en un orden lógico y razonable?
- ¿Está definida sin ambigüedad la responsabilidad de la realización de los controles?
- ¿Pueden realizarse los controles de forma correcta y razonable?
- ¿Son reemplazados los controles híbridos o manuales, en la medida de lo posible, por controles automatizados?
- ¿Los controles detectivos son reemplazados si es posible por controles preventivos?
- ¿Son conformes los controles a las exigencias de las directivas y procedimientos de trabajo?
- ¿Están disponibles las instrucciones e informaciones necesarias para la realización del control?
- ¿Los controles son realizados por una persona cualificada?
- ¿Los controles son realizados con un retraso razonable y con una frecuencia apropiada?
- ¿El diseño de los controles puede ser puesto en marcha en el marco de restricciones organizativas y financieras de la entidad?

En este análisis debe tenerse presente que **los controles automáticos son más eficaces y eficientes que los controles manuales**, pues tienen un funcionamiento continuo en el tiempo y un coste único de implementación. Además, su eficacia es más estable en tanto no se efectúen modificaciones significativas en la aplicación.

Como regla general, una frecuencia elevada de controles manuales o semiautomáticos ocasiona costes y retrasos más elevados respecto a controles automáticos cuya frecuencia no tiene prácticamente influencia sobre los costes de explotación. Por el contrario, una frecuencia de ejecución baja de un control manual o semiautomático puede perjudicar su eficacia.

Está generalmente admitido que **los controles preventivos permiten alcanzar más fácilmente los objetivos de control que los controles detectivos**.

Un control que cubre varios objetivos de control o diferentes riesgos se considera en principio más eficaz, más fiable y más económico que un control centrado sobre un solo riesgo.

En entornos ERP complejos, al evaluar el diseño de controles de aplicación, el auditor debe clarificar las condiciones técnicas requeridas para que el control se desarrolle de la forma prevista. El auditor se planteará principalmente las cuestiones siguientes:

- ¿Puede eludirse o forzarse (rodeo, procedimiento de excepción, superusuario) el control?
- ¿En qué medida depende el control de la parametrización?
- ¿En qué medida depende el control del sistema de derechos de acceso?
- ¿Quién controla el sistema de derechos de acceso?
- ¿En qué medida depende el control de los datos maestros?
- ¿Quién controla los datos maestros?
- ¿Puede registrarse el funcionamiento del control para comprobaciones posteriores (logs, pistas de auditoría)?

8.4 **Procedimientos de auditoría aplicables.** El auditor formará su opinión sobre el **diseño** de los controles:

- Interrogando a los miembros de la dirección de la empresa, a los empleados que tengan tareas de supervisión, así como a los empleados implicados en la realización del control.
- Consultando los documentos relativos a las transacciones y otros documentos importantes de la empresa.
- Observando las actividades específicas de ejecución y de control.
- Siguiendo las transacciones individuales en el sistema de información (mediante las pruebas de recorrido).

8.5 De conformidad con las normas técnicas de auditoría, los procedimientos para la evaluación del diseño de los controles deben estar **respaldados por evidencia de auditoría y adecuadamente documentados**.

Cuando tras una prueba de recorrido y el análisis del diseño de los controles, se llega a la conclusión de que el esfuerzo de auditoría a efectuar para verificar un control clave es desproporcionado, se debe realizar una adaptación de la selección de controles relevantes para hacer un **esfuerzo viable**.

También, al analizar el diseño de los controles, si el auditor identifica controles relevantes que considera inoperantes, el sistema de control evaluado presenta entonces una laguna. Para cubrirla debe identificar otros controles relevantes o **controles compensatorios** y evaluar su eficacia. En este caso, el auditor debe tener presente la selección completa de controles relevantes para evitar crear redundancias costosas en los procedimientos de auditoría.

9. Realización de pruebas del funcionamiento de los controles relevantes

Una vez verificada la razonabilidad y eficacia del diseño de los controles se debe verificar el adecuado funcionamiento operativo de los controles relevantes durante todo el periodo auditado.

Será aplicable la GPF-OCEX 1330.

10. Documentación de la valoración de los riesgos y de la revisión de los controles relevantes

1.01 El diseño de los mapas de procesos o flujogramas, en los que además deben indicarse los principales riesgos y los controles clave (representados por símbolos), debe complementarse con documentos (narrativas) en los que se describan en detalle estos aspectos.

10.2 La documentación debe permitir al auditor comprender cuáles son las "reglas de gestión" que deben ser garantizadas por el control. Además, debe recoger los aspectos ligados al diseño del control desde la perspectiva de su implementación. Deben reflejarse los parámetros o ajustes personalizables para que el control pueda funcionar conforme a las reglas de gestión definidas:

Control relevante		Regla de gestión	Diseño del control
C001	Triple comprobación	No se paga ninguna factura si no concuerdan el pedido, albarán y factura.	
C002	Segregación de funciones	Segregación de funciones entre contabilidad, gestión de deudores y acreedores, tesorería. Las personas que pagan las facturas no pueden crear nuevos proveedores.	

Figura 8 Ejemplo de documentación de controles

Para la comprensión de los controles relevantes de las aplicaciones y, en particular, para la evaluación posterior de su diseño, es importante efectuar una adecuada documentación de los mismos (aunque no es aconsejable una descripción excesivamente detallada de los controles, pues ello acarrearía costes y no generaría un beneficio adicional).

10.3 Para cada proceso de gestión significativo analizado, debe cumplimentarse un formulario de análisis de riesgos en el que debe resumirse el trabajo realizado para identificar y evaluar los riesgos y controles clave relacionados, como el modelo de la figura siguiente.

Se identificarán los epígrafes de las cuentas anuales (capítulo/artículo presupuestario, cuenta y revelación significativa de la memoria), afectados por procesos de gestión (como ingresos, subvenciones, compras y nóminas, etc) y las aplicaciones específicas significativas que afectan a esos capítulos/artículos presupuestarios, cuentas y declaraciones.

Un formulario proporciona una forma práctica y útil de documentar los RIM específicos, que se deben tener en cuenta a la hora de determinar la naturaleza, alcance y momento de ejecución de los procedimientos de auditoría.

En la figura 9 puede verse un modelo de formulario de este tipo.

Formulario de Análisis de Riesgos Entidad: Ayuntamiento de X Y Z	
Proceso de negocio: Subproceso:	*Contratación de inversiones* *Adjudicación*
Cuentas relacionadas:	Capítulo 2, 6 y acreedores
Aplicación informática:	

Riesgo	**Control clave**	**Tipo de control**	**Responsable**	**Eficacia del control**	**Valoración del Riesgo**	**Impacto**
(Describir el riesgo y asignar un identificador secuencial)	(Describir el control y asignar un identificador secuencial. Para cada riesgo puede haber más de un control)	Señalar si es: Manual/Automático Detectivo/Preventivo Compensatorio	(Indicar el responsable del control)	Señalar si es: Efectivo/ No efectivo (en este caso describir la incidencia observada)	Bajo Medio Alto	Describir (señalar la cuenta y la manifestación afectada) y cuantificar (si es posible) cuál podría ser el resultado posible del mal funcionamiento del control
R001-Descripción	C001A-Descripción					
R002-Descripción	C002A -Descripción					
	C002B -Descripción					

Figura 9

11. Evaluación de las incidencias detectadas

11.1 Al revisar la situación de los controles identificados se verificará y documentará su eficacia pudiendo encontrarse cada uno de ellos en alguna de las siguientes situaciones:

Control efectivo

Control bastante efectivo

Control poco efectivo

Control no efectivo

11.2 Las deficiencias de control interno y las recomendaciones que se deriven de las mismas deben estar bien soportadas en los papeles de trabajo. Los hallazgos de auditoría que las soportan deben incluir: (GPF-OCEX 1735; P9)

Criterio (de auditoría): la referencia o norma con la que se compara o evalúa el hecho observado; lo que debería ser.

En las auditorías de sistemas de información (CGTI, controles de aplicación y cibercontroles) los criterios de auditorías son los establecidos con carácter general en la GPF-OCEX relacionadas, que están basadas en el ENS, NIA-ES, ISSAI, etc.

Hecho o condición: la situación observada y documentada en la auditoría.

Están basados en evidencia de auditoría. Pueden ser deficiencias de control, problemas operacionales o incumplimiento de requerimientos legales o administrativos.

Causa: las razones que dan lugar al hecho observado.

Puede servir como base para proponer acciones correctoras en las recomendaciones. Se debe identificar la unidad o departamento responsable de la deficiencia.

Las causas más comunes incluyen políticas, procedimientos o criterios mal diseñados, o aplicados de forma inconsistente, incompleta o incorrecta; o factores más allá del control de los gestores. Los auditores pueden evaluar si la evidencia proporciona un argumento razonable y convincente de por qué la causa indicada es el factor clave que contribuye a la diferencia entre la condición y los criterios.

Efecto: qué consecuencia negativa tiene lugar o podría tener lugar, provocada por la diferencia entre el hecho observado y el criterio.

Explica el impacto adverso al objetivo operacional u objetivo del control. Al articular el impacto y el riesgo, el elemento del efecto real o potencial es muy importante para ayudar a convencer a la administración del auditado de la necesidad de tomar acciones correctoras en respuesta a los problemas y/o riesgos significativos identificados.

Recomendación: acciones correctoras sugeridas.

Las recomendaciones deben redactarse de forma que se aborde la corrección de las causas que originan el hecho o condición observado.

11.3 Al evaluar las deficiencias de control interno detectadas se deben considerar la significatividad de las mismas. En este contexto el concepto “significativo” no puede ser definido de forma exacta, ya que una misma cuestión puede ser significativa, o no, dependiendo de los objetivos de la auditoría y de las circunstancias. *(GPF-OCEX 1735; P10)*

11.4 Las deficiencias de control interno se clasifican en tres niveles de importancia relativa al examinar el control interno: *(GPF-OCEX 1735; P11)*

- Una **deficiencia de control interno** existe cuando el diseño o el funcionamiento de un control no permite al personal de la entidad o a su dirección, en el curso ordinario de las operaciones, prevenir o detectar errores o irregularidades en un plazo razonable. Pueden ser *deficiencia de diseño* del control (cuando un control necesario para alcanzar el objetivo de control no existe o no está adecuadamente diseñado) o *deficiencias de funcionamiento* (cuando un control adecuadamente diseñado no opera tal como fue diseñado o la persona que lo ejecuta no lo realiza eficazmente).
- Una **deficiencia significativa** es una deficiencia en el control interno, o una combinación de deficiencias, que afectan adversamente la capacidad de la entidad para iniciar, autorizar, registrar, procesar o reportar información financiera o presupuestaria de forma fiable, de conformidad con los principios o normas contables y/o presupuestarias aplicables, y existe una probabilidad que es más que remota, de que una manifestación errónea en las cuentas anuales, o un incumplimiento, que no es claramente trivial, no sea prevenida o detectada en plazo oportuno.
- Una **debilidad material** es una deficiencia significativa en el control interno o una combinación de ellas, respecto de las que existe una razonable posibilidad de que una manifestación errónea significativa en las cuentas anuales, incluyendo un incumplimiento de carácter grave, no sea prevenida o detectada y corregida en plazo oportuno.

11.5 La evaluación de importancia relativa o significatividad de las deficiencias incluye consideraciones sobre los siguientes factores de carácter general: la magnitud del impacto, la probabilidad de que ocurra y la naturaleza de la deficiencia. *(GPF-OCEX 1735; P12)*

Implica evaluar, en el contexto de los objetivos de la auditoría, los siguientes factores:

a) La magnitud del impacto se refiere al efecto probable que la deficiencia pudiera tener en el logro de los objetivos de la entidad y se ve afectado por factores como el tamaño, el ritmo y la duración del impacto de la deficiencia. Una deficiencia puede ser más significativa para un objetivo que para otro.

b) La probabilidad de ocurrencia se refiere a la posibilidad de que una deficiencia afecte a la capacidad de una entidad para alcanzar sus objetivos.

c) La naturaleza de la deficiencia implica factores tales como el grado de subjetividad implicado con la deficiencia y si la deficiencia surge del fraude o de una conducta indebida.

11.6 Para determinar si una deficiencia de control, individualmente o junto con otras, constituye una deficiencia significativa o una debilidad material, el auditor considerará varios factores, incluyendo:

- Perjudica o puede perjudicar el cumplimiento de los objetivos de la entidad.
- Es una deficiencia de control interno que ocasiona un aumento significativo del riesgo de auditoria.
- La probabilidad de que una persona pueda obtener acceso no autorizado o ejecutar actividades no autorizadas o inapropiadas en sistemas críticos de la entidad o archivos que puedan afectar a la información con impacto en las cuentas anuales. Esto puede incluir:
  (1) la habilidad para tener acceso a sistemas en los que residen aplicaciones críticas y que posibilita a usuarios no autorizados a leer, añadir, borrar, modificar o extraer información financiera, bien directamente o a través de la utilización de software no autorizado;
  (2) la habilidad para acceder directamente y modificar ficheros que contengan información financiera;
  (3) la habilidad para asignar derechos de acceso a las aplicaciones a usuarios no autorizados, con la finalidad de procesar transacciones no autorizadas.
- La naturaleza de los accesos no autorizados que pueden conseguirse (por ejemplo: limitados a programadores del sistema o de las aplicaciones o a administradores del sistema; a todos los usuarios; a alguien externo a través de acceso no autorizados por Internet) o la naturaleza de las actividades no autorizadas o inadecuadas que pueden llevarse a cabo.
- La probabilidad de que importes de las cuentas anuales estén afectados de forma significativa.
- La probabilidad de que otros controles puedan prevenir o detectar accesos no autorizados.

- El riesgo de que la dirección de la entidad pueda burlar los controles (por ejemplo, mediante derechos de acceso excesivos).

Algunas deficiencias de control pueden ser consideradas no significativas individualmente, pero consideradas juntamente con otras similares, el efecto combinado puede ser más significativo.

11.7 Basándose en las consideraciones reseñadas el auditor informático determinará si las deficiencias de control son, individualmente o en conjunto, debilidades materiales o deficiencias significativas para el adecuado funcionamiento de los sistemas de información.

Si las deficiencias de control constituyen debilidades materiales, el auditor financiero, en base al trabajo del auditor informático, concluirá que los controles internos no son eficaces y deberá replantearse su estrategia de auditoria, es decir, la combinación adecuada de pruebas de cumplimiento y de pruebas sustantivas, dando mayor énfasis a estas últimas para intentar minimizar el riesgo final de auditoria.

11.8 Si se efectúan recomendaciones, existirá una relación directa entre el tipo de deficiencia de control (según su importancia relativa), el riesgo de auditoría que representa, y la prioridad que se conceda a cada recomendación.

La prioridad también estará matizada por consideraciones coste/beneficio.

En el cuadro siguiente se resume la relación existente entre los tres tipos de deficiencias de control según su significatividad o importancia relativa, el riesgo que representan y la prioridad de las recomendaciones correspondientes: *(GPF-OCEX 1735; P13)*

Tipo de deficiencia según su importancia relativa	Riesgo	Prioridad de una recomendación	
Debilidad material	**Alto**	**Alta**	Se requiere atención urgente de la dirección para implantar controles/procedimientos que mitiguen los riesgos identificados.
Deficiencia significativa	**Medio**	**Media**	La dirección debería establecer un plan de acción concreto para resolver la deficiencia observada en un plazo razonable.
Deficiencia de control interno	**Bajo**	**Baja**	

Figura 10

11.9 Las debilidades materiales deben ser incluidas en el informe de auditoría como una salvedad o como una conclusión, según el tipo de informe.

12. Bibliografía

- Global Technology Audit Guide: Auditing Application Controls, julio 2007, The Institute of Internal Auditors.
- COBIT and Application Controls, 2009, ISACA.
- Federal Information Systems Audit Manual (FISCAM), 2009, GAO.
- Manual IDI-WGITA sobre auditoria de TI para las Entidades Fiscalizadoras Superiores, 2013, INTOSAI. 2017 para la traducción española de OLACEFS.

Anexo 1: Identificación de las aplicaciones de gestión significativas (GPF-OCEX 1315, Anexo 2)

a) Identificación de los procesos de gestión significativos

Las cuentas anuales de una empresa o entidad son el resultado de la agregación de múltiples actividades que se pueden agrupar en procesos, y que pueden ser muy diferentes unos de otros.

Partiendo de las clases de transacciones significativas identificadas, el auditor debe identificar los procesos de gestión significativos que influyen en sus importes o en sus saldos contables.

Un **proceso de gestión** (o proceso de negocio) consiste en una serie de actividades, operaciones o funciones (manuales, semiautomáticas o automatizadas) realizadas 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. Pueden clasificarse en tres grupos:

- Procesos relacionados con la **actividad principal** de la entidad: gestión de subvenciones, gestión de historias médicas, matriculación universitaria, compras, ventas, etc.
- Procesos **financieros**: cobros, pagos, nóminas, etc.
- Procesos **de apoyo**: agrupan todas las funciones de apoyo a la puesta en marcha y a la explotación de los procesos operativos, como gestión de recursos humanos, mantenimiento de inventario de inmovilizado, contabilidad, etc.

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. El concepto de materialidad puede ayudar al auditor a determinar qué componentes de las cuentas y que aplicaciones relacionadas son significativas para los objetivos de la auditoría.

Si existieran debilidades de control en los procesos de gestión significativos podría cuestionarse la fiabilidad de las cuentas anuales. Por ello resulta indispensable la identificación minuciosa de los procesos de gestión significativos y de los flujos de procesamiento de datos para poder identificar y valorar los riesgos en el seno de cada uno de ellos. Es decir, se debe:

- Identificar los flujos de datos. Es necesario tener una visión global de la circulación de los datos a lo largo de todo el proceso o procesos analizados, desde su captura inicial, tratamiento, hasta su archivo final. Esto incluye la identificación de las bases de datos que intervienen y las operaciones que se realizan para transferir los datos procesados de una base de datos a otra.
- Identificar los riesgos existentes.
- Identificar los controles. A lo largo del flujo de los datos a través del proceso se establecen una serie de controles sobre la validez, integridad, exactitud, confidencialidad y disponibilidad de los datos.
- Revisar pistas de auditoría (trazabilidad). La finalidad es localizar una información o un dato a partir de otro, resultante de una aplicación informática lógica y físicamente alejada. Así, es posible por ejemplo, a partir del saldo de una cuenta del balance o de un capítulo/artículo presupuestario, obtener un detalle de sus movimientos, y de cada uno de éstos el apunte contable realizado y la referencia a los documentos que originaron el movimiento contable. La ausencia de pistas de auditoría es una debilidad del control interno.

Para comprender mejor la actividad de la entidad es conveniente desagregar los procesos complejos en subprocesos (un **subproceso** o función es un subconjunto de actividades o tareas, realizadas por un empleado o funcionario para llevar a cabo sus responsabilidades, que producen un resultado u output).

Veamos dos ejemplos:

Proceso	*Subprocesos*
Gastos de personal	*Presupuestación*
	Gestión de puestos (RPT)
	Gestión de personas
	Elaboración de la nómina
	Pago nómina
	Contabilización
Concesión de subvenciones	*Inicio*
	Instrucción
	Finalización
	Pago

El análisis a realizar se extiende tanto al proceso contable mismo como al proceso puntual de cierre de las cuentas anuales; a procesos de gestión complejos, como el de impuestos-recaudación o ventas-facturación, que tienen influencia tanto en el flujo financiero como en el de mercancías (en este caso varias cuentas del balance, de la cuenta de pérdidas y ganancias y de la liquidación del presupuesto tienen el mismo proceso como fuente u origen de sus datos) y a los procesos de apoyo, como por ejemplo los del área de recursos humanos.

Los procesos que están interrelacionados y afectan a un grupo de transacciones y cuentas pueden agruparse en ciclos. Agrupar los procesos y aplicaciones de gestión en ciclos puede ayudar al auditor a documentar la auditoría y a diseñar procedimientos que sean eficaces, eficientes y relevantes para los objetivos de la auditoría.

Los procesos pueden ser representados de forma gráfica mediante flujogramas.

Al realizar este análisis se debe aprovechar la documentación descriptiva de los procesos de gestión que exista en la empresa o entidad auditada. Normalmente esta documentación se centra en las actividades y es preciso completarla para cada etapa del proceso con las entradas de datos, los tratamientos de datos y los resultados, así como los roles de los distintos agentes que intervienen.

En general, la documentación de la entidad no señalará los riesgos de los procesos, ni los controles clave, que deberán ser identificados y documentados por el auditor en una fase posterior, al analizar los controles de las aplicaciones.

Comprender la actividad y el funcionamiento de la entidad y de los principales procesos de gestión, incluye entender cómo se emplean las aplicaciones informáticas para soportar los procesos de gestión, ya que varían de una entidad a otra.

b) Qué es una aplicación de gestión significativa

Una aplicación de gestión es una combinación de hardware y software usada para procesar información de la actividad de la entidad y puede dar soporte a uno o varios procesos de gestión; esas aplicaciones informáticas pueden tener una mayor o menor complejidad y grado de integración, según los casos.

La automatización e integración de las distintas fases de los procesos de gestión y de numerosos controles internos en un sistema de información **plantea riesgos inherentes adicionales.** Pueden presentarse, por ejemplo, dificultades para implementar una adecuada segregación de funciones; también, si el nivel de integración es muy elevado y los datos se procesan en tiempo real o si se aplica el principio de "entrada única de datos", se generarán procesos y registros automáticos de transacciones que provocarán que pueda ser imposible que existan controles humanos.

Las aplicaciones de gestión integradas, en particular los ERP, condicionan profundamente la manera de trabajar y determinan la forma en la que se hacen los intercambios entre los distintos agentes que intervienen en un proceso de gestión, contribuyendo a la estructuración de los procesos.

La identificación de las aplicaciones de gestión significativas para los propósitos de la auditoría financiera, el análisis de sus características y de sus interfaces, se debe hacer lo antes posible, ya que esta información permitirá definir de forma detallada el diseño, alcance y la extensión de las pruebas de auditoría, el grado de participación requerido del auditor informático y la elaboración de los programas de auditoría.

Por lo general se considerará que una aplicación es significativa, a los efectos de la auditoría financiera, cuando soporte un proceso de gestión significativo, si 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 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.).

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

De forma gráfica:

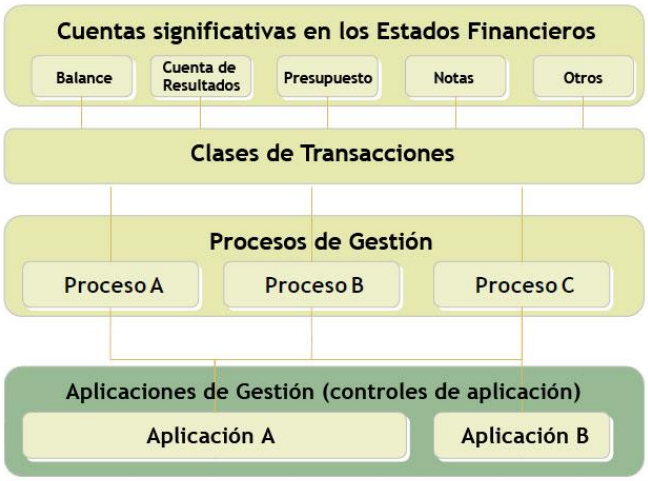


Figura 7

c) Información a obtener sobre las aplicaciones de gestión

El auditor basándose en: a) la información obtenida mediante los cuestionarios, b) entrevistas mantenidas con el personal de la entidad, c) experiencia de años precedentes y d) el análisis de las cuentas anuales junto con otra información obtenida en las etapas iniciales del trabajo, determinará las aplicaciones informáticas que son la fuente para la formación de las cuentas anuales.

Por ejemplo, las aplicaciones que contienen registros auxiliares de las cuentas a cobrar, inmovilizado y cuentas a pagar, por lo general ofrecen información detallada para pruebas y respaldo para los saldos de los libros mayores, si se llevan a cabo unos controles adecuados (por ejemplo: reconciliaciones).

Cuando una cuenta significativa tiene más de una fuente de información financiera, el auditor debe considerar las distintas fuentes y determinar cuál de ellas es más apropiado utilizar para los propósitos de la auditoría financiera. El auditor debe evaluar la probabilidad de que se produzcan incorrecciones y los procedimientos de auditoría que se pueden aplicar al elegir la fuente que va a utilizar.

El auditor debe obtener un conocimiento suficiente de los sistemas de información relevantes para la información financiera para entender el diseño de los procesos. Debe obtener y revisar documentación, como pueden ser documentos de diseño, proyectos, procedimientos de los procesos de gestión, manuales de usuario, etc. Debe también entrevistarse con el personal con conocimientos a fin de obtener una comprensión general de cada aplicación de gestión significativa para los objetivos de la auditoría.

En esta tabla se intentará relacionar las principales cuentas o epígrafes de las cuentas anuales con su correspondiente proceso de gestión, con las aplicaciones de gestión que lo soportan y otros datos relacionados.

Será útil completar una tabla resumen con la información que se muestra la tabla siguiente:

Cuentas anuales		Aplicaciones				Bases de datos		Sistemas operativos		Plataforma hardware
Epígrafe	Importe (Mill. euros)	Proceso	Aplicación utilizada	Tipo de aplicación	Respon-sable	Versión	Adminis-trador	Versión	Respon-sable	

Figura 8

Después de identificar las aplicaciones significativas, debe obtenerse un conocimiento suficiente de las mismas y de los procedimientos (incluyendo los componentes del control interno) mediante los cuales las transacciones son iniciadas, registradas, procesadas y presentadas desde el momento en que acontecen hasta que son incluidas en las cuentas anuales y **documentar** las principales características de cada aplicación significativa, por ejemplo:

- Procedimientos por los que se inician las transacciones, se autorizan, registran, procesan, acumulan y se muestran en las cuentas anuales, incluyendo el tipo de archivos informáticos y la forma en que se puede acceder a ellos, actualizarlos y borrarlos.
- Naturaleza y tipo de los registros, listados contables, documentos fuente y cuentas relacionadas.
- Entorno técnico y sistemas informáticos asociados a cada aplicación.
- Procedimientos para subsanar el procesamiento incorrecto de transacciones.
- Procesos por los que se capturan hechos y condiciones diferentes de los ordinarios.
- Estimación de los volúmenes tratados.
- Tipo de control de acceso.
- Persona responsable de la aplicación.
- Los flujos de transacciones (estudio detallado de los controles internos de la entidad sobre una categoría concreta de hechos que identifica todos los procedimientos y controles clave relacionados con el procesamiento de transacciones), y
- La interacción de la aplicación y software (las transacciones dejan un sistema para ser procesadas por otro, por ejemplo, interfaces de tarjetas de registro horario de personal con el fichero de salarios y complementos para determinar la información de la nómina.

Alcanzar una comprensión de todo esto es fundamental para poder evaluar el riesgo del sistema de información, comprender los controles de aplicación, así como desarrollar los procedimientos de auditoría pertinentes.

d) Documentación del trabajo

El auditor debe preparar suficiente documentación, que describa claramente el sistema de información contable, y que incluya evidencia sobre la implementación de los controles.

Para cada proceso o aplicación significativa, el auditor preparará unas notas descriptivas, que podrán incluir tablas informativas y flujogramas (o mapas de procesos).

Una buena descripción debe:

- Identificar el proceso de gestión y las aplicaciones informáticas que lo soportan.
- Describir las interfaces con otros procesos/aplicaciones
- Identificar los epígrafes de las cuentas anuales, manifestaciones y cuentas afectadas por el proceso.
- Describir las políticas y procedimientos de la entidad relacionadas con el proceso de gestión descrito.
- Identificar (de forma preliminar) los principales controles internos

Se podrán documentar con alguna tabla similar a las vistas en los apartados anteriores.

Será imprescindible elaborar representaciones gráficas de los procesos/aplicaciones, mediante flujogramas. También se podrán utilizar tablas para reflejar información relevante.

Anexo 2 Identificación las principales interfaces *(GPF-OCEX 1315, Anexo 2, apartado 5)*

a) Concepto de interfaz

Un análisis completo de un sistema de información debe tener en cuenta tanto las aplicaciones de gestión como las interfaces.

Una interfaz es una conexión entre dos dispositivos, aplicaciones o sistemas de origen y destino, mediante la que se intercambia información. También se utiliza este término para referirse a la parte de un programa que interactúa con el usuario (la interfaz de usuario), pero este aspecto no interesa en este momento.

El objetivo de esta etapa de la auditoría es comprender los flujos de información y de datos entre distintas funciones, aplicaciones o sistemas, no solo electrónicos sino también manuales. Las interfaces entre aplicaciones y entre bases de datos requieren una atención especial, en particular las relacionadas con aquellas aplicaciones significativas con impacto en las cuentas anuales.

Los entornos TI complejos generalmente requieren interfaces complejas para integrar sus aplicaciones de gestión críticas. Incluso los sistemas ERP muy integrados a menudo requieren complicadas interfaces para otras aplicaciones distribuidas.

Las interfaces suelen ser gestionadas con tecnología middleware, que actúa como un elemento central de comunicación y coordinación para las interfaces. Pueden residir en los mismos sistemas que comunican o en otros diferentes.

En una interfaz, las intervenciones del usuario pueden ser muy variadas:

- integración o exportación de un fichero con descripción del formato de entrada o salida (estos casos más que interfaces, son ficheros de intercambio).
- Desencadenamiento manual de un proceso automático.
- Simple verificación del tratamiento de las excepciones o de los rechazos de la interfaz.

Las interfaces como mínimo mueven información de un sistema a otro, pero también pueden ser responsables de cálculos o de modificar datos de acuerdo con algún algoritmo.

Las interfaces siempre son unidireccionales, nunca bidireccionales.

b) Riesgo de las interfaces

Dado que las interfaces juegan un importante papel en el procesamiento de las transacciones, siempre deben considerarse en el plan de la auditoría. Debe tenerse presente que su mal funcionamiento puede afectar a todo el sistema, lo que representa un riesgo a considerar.

Se deben evaluar los **riesgos de interfaz** (pérdida de datos por interrupción de las comunicaciones, duplicación de datos en el sistema de destino, actualización del sistema de destino con datos de un período incorrecto, etc.) y los controles establecidos para mitigarlos.

Los **controles de interfaz** pueden ser manuales (p.e. mediante reconciliaciones manuales) o estar automatizados (los datos de ambos sistemas se concilian automáticamente).

El **riesgo de interfaz** surge cuando las interfaces externas e internas no son adecuadamente especificadas, definidas, diseñadas, documentadas y programadas. Estos riesgos de interfaz con frecuencia llevan a una reconciliación inconsecuente/desigual de datos enviados y recibidos, teniendo como resultado errores no identificados en los datos. Unas interfaces diseñadas de manera efectiva prevendrán y detectarán estos errores de la forma más rápida posible en el procesamiento. De la misma manera facilitarán la corrección de errores y el empleo de unos controles de usuario apropiados. Cuando las interfaces han sido adecuadamente estructuradas y documentadas, éstas ayudan a conseguir un mantenimiento rentable y una capacidad de recuperación (de datos).

Los riesgos de interfaz se pueden gestionar asegurándose de que no se realizan cambios no autorizados en los datos; transfiriendo los datos a tiempo/de forma periódica, precisa y completa; y llevando a cabo unos procedimientos de resolución de errores con exactitud y oportunamente. Además, el sistema de recepción de los datos debe procesarlos más de una vez como medida preventiva ante posibles riesgos de interfaz.

En el siguiente cuadro se enumeran una serie de ejemplos de objetivos de control específicos y los riesgos y controles relacionados.

OBJETIVO DE CONTROL	RIESGO	CONTROL
Los controles de aplicación son adecuados para preparar o procesar datos enviados y recibidos.	Unos controles inadecuados impiden una disponibilidad de la información de manera exacta y oportuna tanto para la aplicación como para los usuarios de la aplicación heredada.	● Una vez la aplicación recibe los datos, se convierten al formato adecuado; a continuación, la información que ha sido convertida entra en la sesión y los errores quedan registrados. ● Los errores son subsanados y reenviados, y se documentan y son aprobadas las resoluciones. ● Se informa al propietario de la interfaz de los errores que no han sido subsanados.
Los procedimientos de reinicio de proceso y de recuperación de información para las sesiones de interfaz han sido adecuadamente instalados a fin de garantizar que las interrupciones en la transmisión de archivos entre sistemas son resueltas a tiempo.	Unos procedimientos de reinicio de proceso y de recuperación de información mal diseñados pueden ocasionar unos retrasos excesivos en el procesamiento y una pérdida de tiempo innecesaria y costosa del personal.	● Las sesiones de interfaz utilizan una aplicación que cuenta con su propio sistema de reinicio en el caso de que se interrumpa una conexión. ● La aplicación también utiliza un sistema informático de control durante la transferencia de archivos; este sistema es configurable y comprueba las transferencias de datos entre las ubicaciones origen y destino. ● Las transferencias que son interrumpidas o fallan antes de que concluyan son automáticamente reanudadas desde el último control.
Se hace un seguimiento de la información que ha sido transferida entre las aplicaciones y esta información es controlada a fin de asegurar que los errores son subsanados de manera adecuada.	La entrada manual de datos es vulnerable al error humano; sin un seguimiento y un control adecuados, los errores pueden pasar desapercibidos.	Unos controles de edición regulares, incluidas unas reconciliaciones, son responsables de capturar datos incorrectos antes de que se cree un archivo de configuración de la interfaz.

Figura 9

Además, el diseño de la interfaz debe garantizar que se realiza un mapeo adecuado de los datos de origen a una aplicación destino o bien a una tabla de datos, así como una evaluación de los datos/información en lo que refiere al nivel de detalle necesario a utilizar en la aplicación destino.

c) Consideraciones de auditoría sobre las interfaces

Cualesquiera que sean las ventajas de un ERP y la voluntad de una entidad de implantar un sistema integrado, el sistema de información está a menudo constituido de varias aplicaciones heterogéneas. Los procedimientos de auditoría se harán sobre cada una de las aplicaciones, pero también sobre las interfaces que posibilitan la transferencia de datos.

Las interfaces deben ser descritas teniendo cuidado de identificar los aspectos señalados más adelante.

Se debe indagar si existe un módulo específico para la gestión de interfaces. Generalmente existen para las interfaces salientes vía las funcionalidades de exportación de datos. Respecto de la importación de datos, conviene averiguar las funcionalidades que permiten a los usuarios seguir el buen funcionamiento de las interfaces, por ejemplo: el seguimiento de los procesos (situación, cumplimiento de la frecuencia prevista, …), identificación de los posibles rechazos, la posibilidad de conocer la causa de los rechazos y de volver a tratar los datos afectados.

Es necesario identificar el tipo de interfaz que tiene el ERP que se está revisando, en particular para las interfaces entrantes.

Se pueden clasificar las interfaces según cuatro categorías principales:

- Interfaces utilizando un lenguaje o un módulo específicamente propuesto por el fabricante del ERP. Este módulo utiliza generalmente las funciones del ERP; los datos integrados por la interfaz se someten a los mismos controles que los datos registrados manualmente por el usuario.
- Las interfaces que utilizan el lenguaje o un módulo proporcionado por el SGBD. En estos casos, si los datos se someten a los controles propios del SGBD (control de coherencia de datos) no serán sometidos a los controles funcionales de las aplicaciones. Estos controles más ricos pueden afectar por ejemplo a las verificaciones de cálculos (tipo de retención IRPF, tipo IVA, etc.).
- Interfaces que utilizan un lenguaje normalizado, como en el caso de los intercambios EDI.
- Otras interfaces utilizando distintos medios no previstos por el fabricante del ERP (modificación de los programas, escrituras directas en las tablas de la base de datos, …).

La revisión de las interfaces pasa por la comprensión del tipo de interfaz analizada, para identificar los tipos de controles internos aplicados y para detectar los riesgos asociados. Se considera en general que una interfaz estándar situada al nivel de la aplicación presenta pocos riesgos, puesto que los datos integrados que provengan de una aplicación externa se someten a los mismos controles que los datos capturados directamente por la aplicación.

Otros aspectos específicos a considerar son:

- Responsable de la interfaz.

  ¿Quién la inicia?

- Utilización de software para gestionar interfaces.

  ¿El software modifica los datos o solo los traslada de un sitio a otro?

- Interfase IDs: el software de la interfaz probablemente necesitará acceder a los sistemas/aplicaciones que comunica.

  ¿Cómo se gestiona ese acceso?

  ¿Se utilizan identificadores de usuario genéricos?

  ¿Qué privilegios proporcionan esos IDs?

  ¿Quién tiene acceso y puede usar esos IDs?

- Carpetas/directorios de la interfaz.

  ¿Se mueven todos los datos a través de una sola carpeta?

  ¿Quién tiene acceso a esa carpeta?

  ¿Cómo está protegida y controlada?

  ¿Puede algún empleado acceder a esa carpeta para depositar información para procesar? Este aspecto es especialmente crítico cuando se trata de datos sobre pagos o transferencias.

- Tipos de interfaz.

  ¿Qué tipo de interfaz se utiliza?

  ¿Es en tiempo real o de procesamiento por lotes?

  ¿Qué transacciones soporta?

  ¿Inicia el procesamiento de otras transacciones?

d) Procedimientos de auditoría

Si los métodos de revisión varían según el tipo de interfaz, el objetivo es el mismo en todos los casos: se trata de comprobar el funcionamiento de los controles implantados por la entidad (verificación del tratamiento de la interfaz según la frecuencia prevista, seguimiento de los controles realizados sobre los datos, de los rechazos y su tratamiento, etc.).

Los controles de interfaz pueden ser manuales (p.e. mediante reconciliaciones manuales) o estar automatizados (los datos de ambos sistemas se concilian automáticamente).

Se deben evaluar los riesgos de interfaz (pérdida de datos por interrupción de las comunicaciones, duplicación de datos en el sistema de destino, actualización del sistema de destino con datos de un período incorrecto, etc.) y los controles establecidos para mitigarlos.

La interrogación de ficheros y bases de datos utilizando CAAT es un procedimiento que proporciona confianza sobre la integridad de la información transmitida entre distintos sistemas.

e) Documentación de las interfaces

Después de identificar las aplicaciones significativas e interfaces, el auditor debe obtener un conocimiento suficiente de las mismas y de los procedimientos (incluyendo los componentes del control interno) mediante los cuales las transacciones son iniciadas, registradas, procesadas y presentadas desde el momento en que acontecen hasta que son incluidas en las cuentas anuales, y documentar los siguientes aspectos para cada interfaz:

- Tipo (manual o automática).
- Aplicaciones origen (de los datos) y destino.
- Frecuencia de uso (diario, mensual, anual).
- Controles implantados para detectar anomalías.
- Otros aspectos relevantes.

Para su análisis inicial y documentación puede realizarse un inventario de las principales interfaces mediante una tabla:

Nombre de interfaz	Tipo	Aplicaciones		Tipo de flujo	Frecuencia	Listas de error	Evaluación de los riesgos
		Origen	Destino				

Figura 10

Anexo 3 Principales categorías de controles de aplicación o de los procesos de gestión

Los controles de los procesos de gestión, también denominados controles de aplicación, son los controles automatizados y manuales aplicados en el flujo de procesamiento de las transacciones. Se refieren a la completitud, exactitud, validez y confidencialidad de las transacciones y datos durante el procesamiento de las aplicaciones. Operan a un nivel detallado de transacciones o actividades a lo largo del proceso de gestión.

Las áreas específicas de controles de aplicación son:

a) Controles de entrada de datos
b) Controles sobre el procesamiento de datos
c) Controles de salida
d) Controles sobre los datos maestros
e) Segregación de funciones (ver Anexo4)

Aunque no son controles del proceso de gestión, los **controles sobre las interfaces** sí que están en el nivel de las aplicaciones y deben revisarse conjuntamente con aquellos, ya que entrañan riesgos importantes de auditoría. Son aquellos controles que aseguran el procesamiento o trasferencia oportuno, exacto y completo de información entre distintas aplicaciones y/o sistemas.

a) Controles de entrada de datos

Las aplicaciones pueden aceptar la entrada de datos manualmente, o automáticamente vía interfaces que procesan por lotes o integradas en tiempo real con sistemas internos o externos. En todo caso los controles de entrada de datos son muy importantes.

Los principales ***objetivos de control*** son los siguientes:

- La entrada de datos se realiza en tiempo oportuno por personal autorizado o procesos autorizados.
- Los datos introducidos son completos, exactos y válidos.
- Los errores y las anomalías de captura y registro son identificados, documentados, comunicados y corregidos en tiempo oportuno, por personas con la adecuada autorización.
- La confidencialidad de los datos está adecuadamente protegida.

Los ***controles*** que pueden establecerse para alcanzar los objetivos de control son:

- Verificar la exactitud de las correcciones de errores por un servicio o persona independiente.
- Las personas responsables de la captura de datos son identificadas por el sistema.
- Los justificantes de captura proporcionados son exhaustivos y transmitidos en tiempo útil.
- Los justificantes de captura se conservan durante el periodo y en la forma legalmente exigida o pueden ser reconstituidos por la organización.
- Perfiles de competencias para la emisión de documentos contables (p.e. regulación de las firmas) y puesta en práctica de un control de las autorizaciones por sistemas de gestión de acceso.
- Segregación de las funciones de creación y de validación de documentos contables.
- Visé o firma sobre los justificantes de captura de datos.
- Formularios de captura de datos comprensibles y útiles (p.e. con campos predefinidos).
- Procesos de identificación precoz y de tratamiento de los errores e irregularidades.
- Archivo sistemático de los documentos contables.
- Digitalización de los justificantes y conservación adecuada.
- Perfiles de competencias para la captura/registro de las transacciones y puesta en práctica a través de un control de las autorizaciones por sistemas de gestión de accesos.
- Comparación de datos capturados con valores registrados.

- Máscaras de captura comprensibles y amigables con controles de formato de datos integrados (p.e. campos de fecha, numéricos, campos obligatorios, etc., y lista de valores predefinidos y recurrentes).
- Control automático de los valores introducidos (p.e. superación de valores límites, control de factibilidad (credibilidad) de los contenidos, sincronización con los datos archivados).
- Despliegue de etiquetas de código completas después de la grabación del código (p.e. la designación de un artículo se muestra al grabar el número del artículo).
- Totales de control por lotes: número de documentos (p.e. facturas), suma de zonas de valores visibles en los documentos o sumas numéricas (importes, cantidades), suma de control.
- Control secuencial de documentos contables numerados correlativamente para identificar los faltantes o duplicados en las grabaciones.
- Captura de control (llamada también doble captura, control de los 4 ojos); captura doble de valores importantes por diferentes personas o por una misma persona.
- Control visual de valores capturados por una segunda persona; conviene para los casos críticos y un pequeño número de transacciones.
- Proceso de identificación precoz y de tratamiento de errores y de anomalías, las transacciones corregidas deben ser enteramente verificadas de nuevo.
- La exactitud, exhaustividad y la validez de los campos importantes son controlados en las pantallas o programas superpuestos al proceso de captura.

b) Controles sobre el procesamiento de los datos

Una vez que los datos son introducidos en el sistema y aceptados, su procesamiento es controlado por una serie de actividades dentro del sistema. Los pasos del procesamiento son distintos para cada proceso de gestión y los requerimientos de control para mitigar los riesgos inherentes son diferentes en cada caso. Una eficaz evaluación de estos controles incluye una comprensión de las distintas fases del proceso y del flujo de los datos, de los controles embebidos en la aplicación y de los controles manuales existentes en el proceso.

Los principales ***objetivos*** de los controles de procesamiento de datos son los siguientes:

- Las transacciones (cálculos, totalizaciones, consolidaciones, análisis, etc.), incluidas las que genera el propio sistema, son procesadas por el ordenador de forma exacta, completa y oportuna.
- Las transacciones no son objeto de pérdida, duplicación, manipulación o alteración.
- La exhaustividad, exactitud y la validez del procesamiento realizado son verificados según un procedimiento de rutina.
- Los errores de procesamiento son identificados rápidamente, documentados y corregidos en tiempo útil.

Los ***controles*** típicos del procesamiento de datos son los siguientes:

- La aplicación está diseñada para procesar los datos con la mínima intervención manual.
- La separación de funciones está garantizada incluso durante el procesamiento de los datos.
- Las transacciones generadas automáticamente por la aplicación (p.e. intereses periódicos de préstamos, órdenes al sobrepasar umbrales de stocks) son objeto de los mismos controles de exhaustividad, exactitud y de validez que las transacciones aisladas.
- Las decisiones importantes basadas en cálculos automáticos son adoptadas y verificadas por personas.
- Comparación de los datos tratados en el sistema con confirmaciones externas (p.e. inventarios físicos, confirmación de saldos bancarios y de saldos de clientes y proveedores).

c) Controles sobre la salida de los datos

Las salidas u outputs son el resultado del procesamiento de los datos.

Los principales ***objetivos*** de control de la salida de datos son los siguientes:

- Los resultados del procesamiento son completaos y exactos.
- El acceso a los datos de salida del sistema está restringido al personal autorizado.
- Los datos de salida del sistema llegan al personal autorizado en tiempo oportuno, de conformidad con los procedimientos definidos.

Los ***controles*** típicos de la salida de datos son los siguientes:

- Los controles de envío y de recepción regulan las modalidades de comunicación de listados y otros outputs (quién, cuándo, qué, cómo y cuántos ejemplares).
- Los sistemas de gestión de acceso garantizan la trazabilidad de los accesos de los usuarios a consultas en pantalla o a listados.
- Los controles de numeración y de exhaustividad garantizan que la gestión, edición, restitución, recepción y destrucción (p.e. en caso de copia de control) de outputs críticos (p.e. cheques, vales, etc.) se efectúan de conformidad con los procedimientos.
- La exactitud y la completitud de los informes periódicos (p.e. listados semestrales o anuales) son controlados mediante muestreos.

d) Controles sobre los datos maestros

Los datos maestros son los datos permanentes utilizados por múltiples aplicaciones y participan en la correcta ejecución del procesamiento de datos realizados por las aplicaciones. El mantenimiento de su integridad es un elemento crítico para la correcta ejecución de la aplicación.

Ejemplos de datos maestros:

Estructura del plan contable
Maestro de clientes
Maestro de proveedores
Maestro de empleados/nómina
Maestro de materiales (de inventario)
Maestro de bancos

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

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

Los ***controles*** típicos son los siguientes:

- Existen procedimientos para las modificaciones.
- Las actualizaciones se realizan de forma simultánea en todo el sistema de información.
- Sólo las personas autorizadas pueden modificarlos.
- Se mantiene un fichero histórico con todos los cambios en los datos maestros incluyendo quién los realizó.

e) Controles sobre las interfaces

Raras veces una organización utiliza un único sistema para gestionar todos sus procesos e información. Las interfaces se crean para permitir a la información pasar de una aplicación o sistema a otro.

Las características de las **interfaces** afectan a la evaluación del riesgo. Las manuales presentan un mayor riesgo de errores (de captura de datos, omisión de operaciones, duplicados, etc.) que las automáticas. En las interfaces automáticas debe comprobarse la existencia de logs o informes que permitan

comprobar la correcta ejecución del procesamiento (informes de anomalías, informes de ejecución que permitan comparar los datos que entran y salen de la interfaz); los informes deben ser analizados y dar lugar a las acciones correctoras que procedan.

La fiabilidad de una interfaz se analiza estudiando las condiciones de implementación, de funcionamiento y de actualización. A priori una interfaz nueva, no testeada completamente, tiene más posibilidades de funcionar mal.

Las interfaces de entrada y de salida de una aplicación deben ser consideradas como fuentes de riesgo. Es muy importante identificarlas y revisarlas (ver Anexo 2).

Los controles de interfaz son aquellos diseñados para el procesamiento de información oportuno, exacto y completo entre aplicaciones y otros sistemas emisores y receptores de información.

Los principales **objetivos** de control relativos a las interfaces son los siguientes:

- Implementar una estrategia y diseño eficaces.
- La interfaz se ejecuta completamente, con exactitud, solo una vez, y en el periodo adecuado.
- Los errores de la interfaz son rechazados, identificados y corregidos con prontitud.
- El acceso a los datos y procesos de la interfaz está adecuadamente restringido. Los datos son fiables y se obtienen únicamente de fuentes autorizadas.
- La autenticidad y la integridad de las informaciones provenientes de fuentes externas a la organización son controladas cuidadosamente antes de emprender cualquier acción potencialmente crítica, independientemente del medio de recepción (teléfono, fax, email, etc.).
- Las informaciones sensibles están protegidas durante su transmisión por medidas adecuadas contra accesos no autorizados, modificaciones o envío a destinatarios erróneos.

Los ***controles*** típicos al nivel de las interfaces son los siguientes:

- Existe una estrategia y diseño para cada interfaz que incluye:
  - tipo
  - campos de datos a transferir
  - controles de integridad y exactitud
  - programación temporal
  - responsable
  - requisitos de seguridad
  - corrección de errores
  - método de comunicación
- Los archivos generados por una interfaz (entrante o saliente) son adecuadamente protegidos contra accesos no autorizados o modificaciones.

  Un ejemplo típico es el fichero (C34) generado por la aplicación de pagos para su remisión telemática a las entidades financieras. Tras su generación se archiva en una carpeta del sistema de la entidad, antes de su envío al banco. Un control de interfaz saliente consiste en proteger ese fichero y esa carpeta para que nadie no autorizado pueda acceder al fichero editable C34 y modificarlo fraudulentamente.
- Existen procedimientos para asegurar que todos los archivos enviados por el sistema origen han sido recibidos por el sistema destino.
- Los datos transmitidos son reconciliados entre las aplicaciones de origen y destino para asegurar que la interfaz es completa y exacta. Los totales de control coinciden y los listados de conciliación proporcionan suficiente información para conciliar cada transacción procesada.

Los controles de interfaz pueden realizarse manual o automáticamente, de forma programada o esporádica, electrónicamente o en papel. Los controles más fiables son los automatizados.

Anexo 4 Segregación de funciones (SdF)

Al revisar un proceso/aplicación 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 procesamiento 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 y/o autorización de este último.

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

En la práctica, este principio de segregación de 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.

En los actuales sistemas altamente automatizados, en los que los usuarios tienen acceso potencialmente a todas las funciones del sistema, el análisis de la segregación de funciones adquiere una importancia crítica y debe hacerse una detallada revisión de los riesgos existentes en la gestión de los permisos de acceso a las aplicaciones y bases de datos subyacentes (ambos niveles deben analizarse de forma inseparable).

Dada su complejidad y "no visibilidad", en los sistemas informatizados, el análisis de la segregación de funciones muchas veces **solo será posible realizarlo** con la colaboración de personal especializado utilizando técnicas de auditoría de sistemas.

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

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

Una adecuada SdF contemplará, por ejemplo:

- Ningún empleado tendrá responsabilidad total para modificaciones en los Ficheros Maestros de Precios y de Condiciones de Ventas. Un empleado iniciará el cambio y otro revisará y autorizará el cambio.
- Los empleados que tengan capacidad de modificar los Ficheros Maestros no deben intervenir en la gestión de las ventas.
- Los empleados/responsables que venden entradas no son los mismos que están en la entrada cancelando las entradas o vigilando la entrada.
- Los empleados/responsables de la gestión comercial/venta de entradas son distintos a los que supervisan las cuentas bancarias que recogen las ventas en efectivo o con TPV.
- Ningún empleado tendrá responsabilidad total para modificaciones en el FME (Fichero Maestro de Empleados). Un empleado iniciará el cambio y otro revisará y autorizará el cambio.
- Los empleados que tengan capacidad de modificar el FME no deben intervenir en la elaboración de la nómina.

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. En las empresas y entidades de mayor tamaño, las posibilidades de desagregación del trabajo en los procesos de gestión son mayores, pero 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[7] que pueden ayudar a mitigar la gravedad de las debilidades de control, por ejemplo:

- Un supervisor que no interviene en la elaboración de la nómina, revisa y aprueba los ficheros de la nómina antes y después de su cálculo definitivo.
- Se utilizan herramientas analíticas (como ACL) para verificar la exactitud de los salarios reconciliándolos con los tc'1, Mod110 y Mod190.
- Si un empleado que participa en la elaboración de la nómina también mantiene el FME, se debería generar un informe de todos los cambios en el FME para que fueran supervisados por una persona independiente.

Para facilitar la revisión de la SdF existente en una entidad, es conveniente utilizar un cuadro como el del ejemplo siguiente en el que se recojan las principales situaciones de falta de segregación de funciones en el proceso auditado, que pueden entrañar riesgos de errores o irregularidades, y por tanto riesgos de auditoría.

Función	Consideraciones de control / Preguntas de auditoría	Control	Controles compensatorios

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

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.

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