GPF-OCEX 5340 Revisión de los controles de procesamiento de la información (CPI) en un entorno de administración electrónica

Referencia: GPF-OCEX 1315R, GPF-OCEX 1316R y GPF-OCEX 5330

Documento elaborado por la Comisión Técnica de los OCEX y
aprobado por la Conferencia de Presidentes de ASOCEX el 26/06/2024

*La Conferencia de Presidentes de los OCEX aprobó el 12/11/2018 la primera versión de la **GPF-OCEX 5340 Los controles de aplicación: qué son y cómo revisarlos**. Han transcurrido más de cinco años desde entonces y en este tiempo se ha producido la entrada en vigor de la NIA-ES 315R/GPF-OCEX 1315R que afecta de forma importante al contenido de la guía y junto con la experiencia adquirida durante estos años en su aplicación práctica han dado lugar a la nueva versión contenida en el presente documento. No obstante, hay que destacar que, a pesar de los numerosos e importantes cambios y adaptaciones, los conceptos esenciales y los principales procedimientos de auditoría se mantienen plenamente vigentes, por lo que la transición entre ambas versiones de la guía no debe plantear ningún problema importante a los auditores de los OCEX que ya aplicaran la versión anterior.*

Para la adecuada comprensión de esta guía deben leerse previamente las GPF-OCEX 1315R y GPF-OCEX 1316R a las que no sustituye, sino que las desarrolla para facilitar su aplicación práctica.

*Junto con esta guía también se ha actualizado la complementaria **GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica,*** con la que está totalmente interrelacionada y hay que conocer simultáneamente.

1. Introducción

El enfoque de auditoría basado en el análisis de los riesgos es el fundamento central de la actividad auditora desarrollada de acuerdo con las Normas Internacionales de Auditoría (NIA-ES) y las ISSAI-ES. 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 gran 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.

En una auditoría financiera basada en el análisis de los riesgos, el estudio y revisión de los sistemas de información que sustentan la gestión de una entidad es una actividad de importancia fundamental, 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) derivados del uso de las TI que se han unido a los riesgos tradicionales que el auditor debe identificar y valorar para determinar cuáles de ellos son riesgos significativos. A continuación, el auditor debe identificar los controles de procesamiento de la información que hacen frente a esos riesgos y diseñar los procedimientos posteriores de auditoría (pruebas de controles y procedimientos sustantivos) acordes con las circunstancias, con la finalidad de minimizar el riesgo de auditoría.

En definitiva, en un entorno de administración electrónica, la revisión de los controles de procesamiento de la información (CPI) y de los controles generales de tecnologías de información (CGTI) que los respaldan es un procedimiento indispensable para reducir los riesgos de auditoría a un nivel aceptable.

En un entorno informatizado de complejidad media o alta, la revisión de los CPI requerirá la colaboración de especialistas en auditoría de sistemas de información, bien personal propio del OCEX o bien expertos externos contratados, y la aplicación de una metodología específica como la recogida en esta guía.

Este documento se centra en la identificación, análisis y revisión de los CPI, y su finalidad es ayudar al auditor a:

- Identificar y valorar los riesgos inherentes en las afirmaciones.
- Determinar los riesgos significativos en el espectro de riesgo inherente.
- Identificar, analizar y revisar el adecuado diseño, implementación y funcionamiento de los CPI relevantes, tanto en las aplicaciones informáticas como en las interfaces relacionadas.
- Valorar el riesgo de control.
- Reducir el riesgo de auditoría a un nivel aceptable.
- Identificar deficiencias de control interno.
- Formular recomendaciones para subsanar las deficiencias de control interno.

Estos procesos son regulados, principalmente, por o están relacionados con las siguientes normas técnicas:

- NIA-ES 315R/GPF-OCEX 1315 Identificación y valoración del riesgo de incorrección material (Revisada).
- GPF-OCEX 1316 Guía de implementación por primera vez de la GPF-OCEX 1315 (Revisada).
- NIA-ES-SP 1330 Respuestas del auditor a los riesgos valorados.
- GPF-OCEX 5330 Revisión de los CGTI en un entorno de administración electrónica.

Además de en las auditorías financieras, la guía también será de utilidad en auditorías de cumplimiento y operativas en las que la gestión auditada está sustentada por sistemas informáticos y se plantean necesidades similares a las auditorías financieras. Por ejemplo, auditar el área de subvenciones requerirá revisar el adecuado funcionamiento del control interno, incluyendo los CPI, ya que entre los objetivos de los CPI está el de cumplimiento de la legalidad.

Cualquier referencia a una auditoría financiera en la guía deberá entenderse realizada también a otros tipos de auditoría adaptándose a las circunstancias particulares de cada trabajo.

2. Definiciones

A efectos de las NIA-ES/GPF-OCEX, los siguientes términos tienen los significados que figuran a continuación:

(a) ***Afirmaciones**:* manifestaciones, explícitas o no, con respecto al reconocimiento, medición, presentación y revelación de información en los estados financieros que son inherentes a la manifestación de la dirección de que los estados financieros se preparan de conformidad con el marco de información financiera aplicable. El auditor utiliza las afirmaciones para considerar los distintos tipos de incorrecciones potenciales que pueden existir al identificar, valorar y responder a los riesgos de incorrección material.

Al identificar, valorar y responder a los riesgos de incorrección material, los auditores utilizan categorías de afirmaciones para considerar los distintos tipos de incorrecciones potenciales que pueden existir. Algunos ejemplos de esas categorías de afirmaciones se describen en el apartado A190 de GPF-OCEX 1315R y 44 de la GPF-OCEX 1316R.

(b) ***Afirmaciones relevantes***: una afirmación sobre un tipo de transacción, saldo contable u otra revelación de información **es relevante cuando tiene un riesgo identificado de incorrección material**. La determinación de si una afirmación es relevante se realiza antes de tener en cuenta los posibles controles correspondientes (es decir, solo se tiene en cuenta el riesgo inherente). Si una afirmación no tiene un riesgo identificado de incorrección material, no se trata de una afirmación relevante.

"Afirmación significativa" y "afirmación relevante" tienen el mismo significado.

(c) ***Tipos de transacciones****:* se refieren a las derivadas de actividades de funcionamiento ordinario o de explotación (básicamente ingresos, compras de bienes y servicios, y las del personal), de inversión o de financiación. Suelen ser repetitivas y, a efectos de auditoría, los procedimientos para su gestión pueden agruparse en ciclos o procesos desde su inicio hasta la terminación.

(d) ***Tipos de transacciones, saldos contables o información a revelar significativos (TTSCIRS)****:* un tipo de transacción, saldo contable o información a revelar para el que existen una o varias afirmaciones significativas o relevantes (es decir afirmaciones en las que existe un RIM).

(e) ***Sistema de control interno***: el sistema 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. A los efectos de las NIA, el sistema de control interno comprende cinco componentes interrelacionados:

- el entorno de control;
- el proceso de valoración del riesgo por la entidad;
- el proceso de la entidad para el seguimiento del sistema de control interno;
- el sistema de información y comunicación y
- las actividades de control.

(f) ***Controles****:* políticas o procedimientos que establece una entidad para alcanzar los objetivos de control de la dirección o de los responsables del gobierno de la entidad. En este sentido:

- ***Políticas*****:** son declaraciones de lo que se debería o no se debería hacer dentro de la entidad para llevar a cabo el control.

  Esas declaraciones pueden estar documentadas, formuladas explícitamente en comunicados o implícitas en actuaciones y decisiones. Son implementadas a través de las actuaciones del personal dentro de la entidad o a través de restricciones que impiden al personal llevar a cabo actuaciones que entrarían en conflicto con esas políticas.
- ***Procedimientos*****:** son actuaciones para implementar las políticas.

  Pueden ser exigidos mediante documentación formal u otra comunicación de la dirección o de los responsables del gobierno de la entidad, o pueden ser el resultado de comportamientos que no se exigen, sino que están condicionados por la cultura de la entidad. Los procedimientos se pueden aplicar mediante actuaciones permitidas por las aplicaciones de TI utilizadas por la entidad o por otros aspectos de su entorno de TI.

  Son un conjunto organizado de actividades que tiene un principio y fin delimitados, que implica recursos y da lugar a un resultado. Abordan tareas concretas, indicando lo que hay que hacer, paso a paso. Detallan de forma clara y precisa cómo llevar a cabo el CPI, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos. En muchas ocasiones estarán total o parcialmente automatizados.

En materia de seguridad, el Esquema Nacional de Seguridad (ENS) establece tres niveles de normas internas: políticas de seguridad, normas y procedimientos.

(g) ***Controles generales de las tecnologías de la información (CGTI)***: controles de los procesos de TI de la entidad que apoyan el funcionamiento continuo apropiado del entorno de TI, incluido el funcionamiento continuo efectivo de los controles de procesamiento de la información y la integridad de la información (es decir, la completitud, exactitud y validez de la información) en el sistema de información de la entidad.

(h) ***Controles del procesamiento de la información (CPI)***: controles relacionados con el procesamiento de la información en aplicaciones de TI o procesamientos manuales de la información en el sistema de información de la entidad que **responden directamente a los riesgos** para la integridad de la información (es decir, la **completitud**, **exactitud** y **validez** de las transacciones y otra información) y el **cumplimiento de la legalidad**.

(i) ***Control compensatorio***: es aquel que reduce el riesgo de una deficiencia de control, real o potencial, no eliminada por un control directo.

(j) ***Control correctivo:*** si han fallado los controles preventivos y ha sucedido un incidente o un desastre, permite recuperarse.

(k) ***Controles detectivos:*** detectan e informan de la ocurrencia de un error, omisión o acto malintencionado.

(l) ***Controles directos:*** son controles lo suficientemente precisos para responder a riesgos de incorrección material en las afirmaciones.

(m) ***Controles indirectos:*** son controles que sustentan los controles directos.

(n) ***Controles preventivos:*** su finalidad es prevenir que ocurra un hecho que no es consistente con los objetivos de control. Detecta los problemas antes de que sucedan.

(o) ***Controles relevantes:*** son aquellos controles que hacen frente (previenen, detectan o corrigen) a los riesgos significativos. Son los que interesan al auditor.

(p) ***Procedimientos de valoración del riesgo***: procedimientos de auditoría diseñados y aplicados para identificar y valorar los riesgos de incorrección material, debida a fraude o error, tanto en los estados financieros como en las afirmaciones concretas contenidas en estos.

(q) ***Procesos de negocio o de gestión de una entidad:*** 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.

Incluyen las actividades diseñadas para: *(párrafo 16 del Anexo 3 de la NIA-ES 315R)*

- el desarrollo, adquisición, la producción, la venta y la distribución de los bienes y servicios de una entidad;
- asegurar el cumplimiento de las disposiciones legales y reglamentarias y
- registrar la información, incluida la información contable y financiera.

Los procesos de negocio tienen como resultado transacciones registradas, procesadas y notificadas mediante una aplicación TI.

(r) ***Aplicación de TI*****:** es un programa o un conjunto de programas que se utiliza para el inicio, procesamiento, registro e información de transacciones o información. Las aplicaciones de TI incluyen almacenes de datos y generadores de informes.

(s) ***Aplicación de TI significativa:*** aunque es un concepto no explícitamente contemplado en la NIA-ES 315R, a efectos prácticos consideraremos como tales aquellas aplicaciones TI que procesan TTSCIR significativas.

(t) El **Sistema de información** relevante para la preparación de los estados financieros consiste en actividades y políticas, y en registros contables y auxiliares, diseñados y establecidos para:

- iniciar, registrar y procesar las transacciones de la entidad (así como los procesos para capturar, procesar y revelar información sobre hechos y condiciones distintas de transacciones), así como para rendir cuentas sobre los activos, pasivos y patrimonio neto correspondientes;
- resolver el procesamiento incorrecto de transacciones, por ejemplo, ficheros de espera automatizados y procedimientos aplicados para reclasificar oportunamente las partidas pendientes de aplicación;
- procesar y dar cuenta de elusiones del sistema o evitación de los controles;

- incorporar información procedente del procesamiento de las transacciones en el mayor (por ejemplo, transferir transacciones acumuladas desde un auxiliar);
- capturar y procesar información relevante para la preparación de estados financieros sobre los hechos y las condiciones distintos de las transacciones, tales como la amortización de activos, así como los cambios en la recuperabilidad de los activos; y
- asegurar que se recoge, registra, procesa, resume e incluye adecuadamente en los estados financieros la información que el marco de información financiera aplicable requiere que se revele.

(u) ***Entorno de las TI*:** las aplicaciones de TI y la infraestructura que da soporte a las TI, así como los procesos y el personal involucrado en esos procesos que una entidad utiliza para respaldar las operaciones de negocio y para lograr la consecución de las estrategias de negocio. A los efectos de esta guía:

- Una **aplicación de TI** es un programa o un conjunto de programas que se utiliza para el inicio, procesamiento, registro e información de transacciones o información. Las aplicaciones de TI incluyen almacenes de datos y generadores de informes.
- La **infraestructura de TI** comprende la red, los sistemas operativos y las bases de datos y el hardware y software relacionados con estos.
- Los **procesos de TI** son los procesos de la entidad para la gestión del acceso al entorno de TI, de cambios en los programas, de cambios al entorno de TI, así como de las operaciones de TI.

(a) ***Riesgo de incorrección material (RIM):*** a efectos de las NIA, existe un riesgo de incorrección material cuando hay una posibilidad razonable de que: (a) exista una incorrección (es decir, su probabilidad de existir); y (b) en caso de que exista, sea material (es decir, su magnitud).

(v) ***Riesgos derivados de la utilización de TI:*** exposición de los controles de procesamiento de la información a un diseño o un funcionamiento ineficaces, o riesgos para la integridad de la información (es decir, la completitud, exactitud y validez de las transacciones y demás información) en el sistema de información de la entidad, debido a un diseño o a un funcionamiento ineficaz de los procesos de TI de la entidad (véase entorno de TI).

(b) ***Riesgo significativo: un riesgo identificado de incorrección material,*** para el que:

- la valoración del riesgo inherente se encuentra próxima al límite superior del espectro de riesgo inherente debido al grado en el que los factores de riesgo inherente afectan a la combinación de la **probabilidad** de que exista una incorrección y a la **magnitud** de la incorrección potencial si existe; o
- debe ser tratado como riesgo significativo de conformidad con los requerimientos de otras NIA.

(c) ***Espectro del riesgo inherente:*** es el grado en que varía el riesgo inherente. Sirve para ayudar al auditor a aplicar su juicio profesional al determinar la significatividad de un riesgo combinando la probabilidad de que exista una incorrección (considerando los factores de riesgo inherente) y de su magnitud.

3. Objetivos y alcance de la revisión de los CPI

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

El **alcance** de la revisión vendrá determinado por el auditor de acuerdo con su necesidad de obtener confianza sobre el funcionamiento efectivo de los CPI relevantes. Para ello se seguirá la metodología descrita en los apartados siguientes de la guía. No se requiere que el auditor identifique y evalúe todos los CPI de un proceso de gestión o aplicación TI, **se centrará en los que responden a los riesgos significativos en las afirmaciones**.

El proceso auditor sigue el esquema que se muestra en la figura 1. No obstante, debe tenerse en cuenta que ese esquema solo refleja el proceso teórico, y en la práctica algunos pasos no son siempre sucesivos, pueden ser simultáneos, en otros casos varios pasos diferenciados en el esquema se realizan simultáneamente, y como señala la NIA-ES 315R el proceso de identificación y valoración de los riesgos por el auditor es iterativo y dinámico. *(Apartado 7)*.

Los destinatarios de la guía serán los miembros de los equipos de fiscalización que deban planificar y ejecutar una auditoría financiera y/o una auditoría de cumplimiento u operativa.

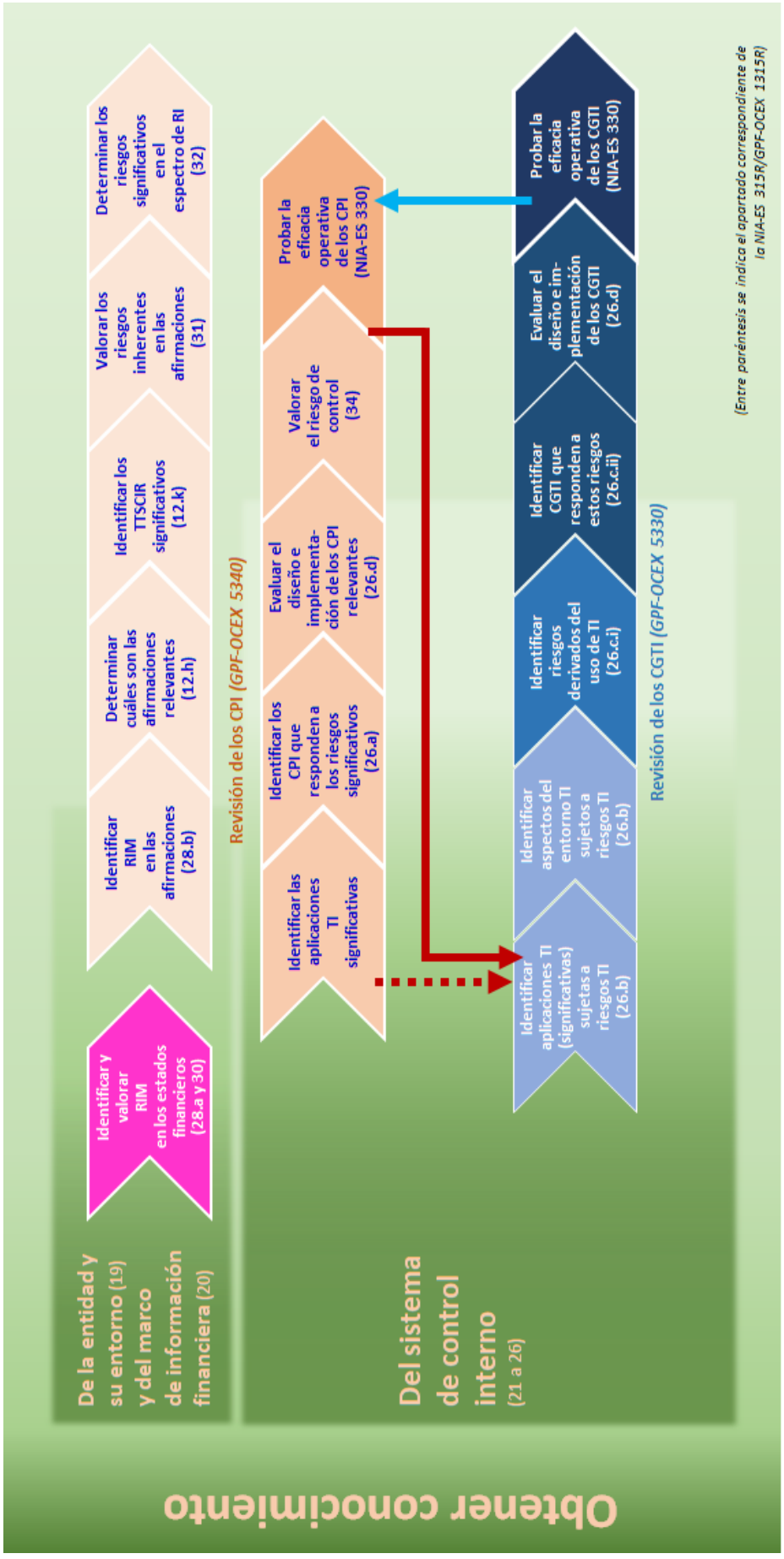
Obtener conocimiento
De la entidad y su entorno (19) y del marco de información financiera (20)
Identificar y valorar RIM en los estados financieros (28.a y 30)
Identificar RIM en las afirmaciones (28.b)
Determinar cuáles son las afirmaciones relevantes (12.h)
Identificar los TTSCIR significativos (12.k)
Valorar los riesgos inherentes en las afirmaciones (31)
Determinar los riesgos significativos en el espectro de RI (32)
Revisión de los CPI (GPF-OCEX 5340)
Del sistema de control interno (21 a 26)
Identificar las aplicaciones TI significativas
Identificar los CPI que responden a los riesgos significativos (26.a)
Evaluar el diseño e implementación de los CPI relevantes (26.d)
Valorar el riesgo de control (34)
Probar la eficacia operativa de los CPI (NIA-ES 330)
Identificar aplicaciones TI (significativas) sujetas a riesgos TI (26.b)
Identificar aspectos del entorno TI sujetos a riesgos TI (26.b)
Identificar riesgos derivados del uso de TI (26.c.i)
Identificar CGTI que responden a estos riesgos (26.c.ii)
Evaluar el diseño e implementación de los CGTI (26.d)
Probar la eficacia operativa de los CGTI (NIA-ES 330)
Revisión de los CGTI (GPF-OCEX 5330)
(Entre paréntesis se indica el apartado correspondiente de la NIA-ES 315R/GPF-OCEX 1315R)

Figura 1

4. Obtención de conocimiento de la entidad y su entorno, del marco de información financiera aplicable y del sistema de control interno de la entidad

(Apartados 19 a 27 de la NIA-ES 315R)

4.1 Obtención de conocimiento

El primer paso de cualquier auditoría será obtener conocimiento de la entidad y su entorno, del marco de información financiera aplicable y del sistema de control interno En la NIA-ES 315R, **hay tres áreas principales que requieren el conocimiento del auditor:**

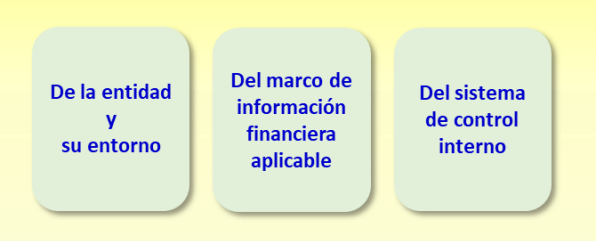

Figura 2

Este es un proceso dinámico e iterativo de recopilación, actualización y análisis de información durante toda la auditoría. Las expectativas del auditor pueden cambiar a medida que se obtiene nueva información.

Esta etapa inicial de una auditoría se explica en detalle en el apartado III de la *GPF-OCEX 1316 Guía de implementación por primera vez de la GPF-OCEX 1315 (Revisada)*, en particular, el **conocimiento de la entidad y su entorno** se trata en el apartado 16 de esa guía y **el conocimiento del marco de información financiera aplicable** en su apartado 17. El conocimiento del control interno se trata con un cierto detalle en el apartado 3 y siguientes de la GPF-OCEX 5330 y en el apartado 6 siguiente.

4.2 Conocimiento de los factores de riesgo inherente (FRI) *(Apartado 15 de la GPF-OCEX 1316R)*

El auditor debe aplicar procedimientos de valoración del riesgo para obtener conocimiento del modo y el grado en que los FRI afectan a la susceptibilidad de las afirmaciones a incorrección en la preparación de los estados financieros de conformidad con el marco de información financiera aplicable.

Los FRI se tendrán en cuenta al valorar el riesgo inherente. El auditor considerará el grado en que los FRI afectan a la susceptibilidad de las afirmaciones relevantes a la incorrección, es decir, puede ayudar a que el auditor considere si la valoración del riesgo inherente para un RIM identificado a nivel de afirmación debe ser mayor o menor en el espectro de riesgo inherente.

Los FRI son características de hechos o condiciones que afectan a la susceptibilidad a incorrección de una afirmación sobre un TTSCIR, debida a fraude o error, antes de considerar los controles. Dichos factores pueden ser **cualitativos o cuantitativos** e incluyen complejidad, subjetividad, cambio, incertidumbre o susceptibilidad de incorrección debida a sesgo de la dirección u otros factores de riesgo de fraude en la medida en la que afectan al riesgo inherente.

En la obtención de conocimiento de la entidad y su entorno, y del marco de información financiera aplicable y de las políticas contables de la entidad de conformidad con los apartados 19(a)–(b) de la GPF-OCEX 1315 Revisada, el auditor también comprende el modo en que los FRI afectan a la susceptibilidad de las afirmaciones a incorrección en la preparación de los estados financieros.

En el anexo 2 se hacen consideraciones adicionales, se describen los FRI y se proporcionan ejemplos de hechos y condiciones que pueden indicar la existencia de RIM en las afirmaciones.

Cuanto mayor sea el grado de susceptibilidad de incorrección material de un tipo de transacciones, saldo contable o información a revelar debida a complejidad o subjetividad, mayor será la necesidad del auditor de aplicar escepticismo profesional.

4.3 El sistema de control interno

(Apartado 20 de la GPF-OCEX 1316R y Anexo 3. Conocimiento del sistema de control interno de la entidad de la NIA-ES 315R/GPF-OCEX 1315R.)

El auditor debe aplicar procedimientos de valoración del riesgo (**PVR**) y adquirir un conocimiento del sistema de control interno que le permitan identificar y valorar los riesgos de incorrección material (**RIM**).

En la GPF-OCEX 1315R se define el sistema de control interno como el sistema 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 sistema de control interno tiene los siguientes cinco componentes:

Figura 3

Para no reiterar el mismo contenido y comprender los siguientes apartados de esta guía **deben leerse los apartados 3 a 6 de la GPF-OCEX 5330.**

El sistema de control interno de la entidad contiene controles manuales y automatizados cuya combinación varía según la naturaleza y complejidad de la utilización de las TI por la entidad. La utilización por la entidad de las TI afecta al modo en que la información relevante para la preparación de los estados financieros se procesa, almacena y comunica y, en consecuencia, afecta al modo en que se diseña e implementa el sistema de control interno de la entidad.

El apartado A94 de la NIA-ES 315R/GPF-OCEX 1315R señala que el objetivo global y el alcance de una auditoría no son diferentes si una entidad opera en un entorno mayoritariamente manual, un entorno totalmente automatizado o un entorno en el que se combinan elementos manuales y automatizados.

Sin embargo, aunque el objetivo y el alcance de una auditoría no sean diferentes, **el grado de digitalización de la entidad, además de a los riesgos, afecta a la forma en que debe realizarse el conocimiento del sistema de control interno y de sus componentes,** a la valoración de los riesgos de control y a los procedimientos posteriores de auditoría basados en dicha valoración.

5. Identificación y valoración de los RIM *(párrafo 28 y siguientes de la NIA-ES 315R)*

El auditor identificará y valorará los riesgos de incorrección material en:

- los estados financieros, y
- las afirmaciones sobre TTSCIR que le proporcionen una base para el diseño y la realización de los procedimientos de auditoría posteriores.

5.1 Identificación y valoración de RIM en los estados financieros *(párrafo 30 de la NIA-ES 315R)*

Se deberá **identificar y valorar los RIM en los estados financieros con la finalidad de:**

a) determinar si dichos riesgos afectan a la valoración de riesgos en las afirmaciones y

b) evaluar la naturaleza y extensión de su efecto generalizado sobre los estados financieros.

Los RIM en los estados financieros **se refieren a los riesgos que se relacionan generalizadamente con los estados financieros en su conjunto y que pueden afectar a muchas afirmaciones** (por ejemplo, si la administración no

es competente, esto afectará de forma generalizada a los estados financieros o, en especial, si el entorno de control es deficiente).

La NIA-ES 315R hace hincapié en los riesgos en los estados financieros y explica el vínculo entre los RIM en los estados financieros y en las afirmaciones. Esto se debe a que el auditor debe determinar si los riesgos identificados tienen un efecto generalizado en los estados financieros y, por lo tanto, **requerirían una respuesta global** de acuerdo con la NIA-ES 330.

Los riesgos en los estados financieros también pueden afectar a las afirmaciones individuales y, por lo tanto, también pueden ayudar a determinar los **procedimientos posteriores** de auditoría para abordar los riesgos identificados en las afirmaciones.

La identificación de los riesgos en los estados financieros se ve influenciada por:

(a) El conocimiento por parte del auditor del **sistema de control interno** de la entidad, en particular la evaluación e identificación de deficiencias en los controles indirectos.

(b) Susceptibilidad a la incorrección debido a factores de **riesgo de fraude** que afectan al riesgo inherente.

En el caso de entidades del sector público, la identificación de riesgos incluirá la consideración de cuestiones relacionadas con el clima político, el interés público y lo sensibles que sean los programas *(Apartado A200 de la NIA-ES 315R).*

Posteriormente se identificarán y valorarán los RIM en las afirmaciones.

5.2 Identificación y valoración de los RIM en las afirmaciones

El RIM en las afirmaciones tiene dos componentes:

- **Riesgo inherente (RI):** susceptibilidad de una afirmación sobre un tipo de transacción, saldo contable u otra revelación de información a una incorrección que pudiera ser material, ya sea individualmente o de forma agregada con otras incorrecciones, antes de tener en cuenta los posibles controles correspondientes.
- **Riesgo de control (RC)**: riesgo de que una incorrección que pudiera existir en una afirmación sobre un tipo de transacción, saldo contable u otra revelación de información, y que pudiera ser material, ya sea individualmente o de forma agregada con otras incorrecciones, no sea prevenida, o detectada y corregida oportunamente, por el sistema de control interno de la entidad.

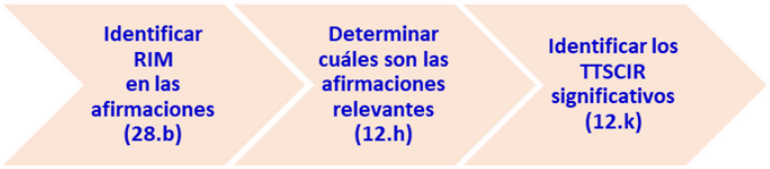

Figura 4

La identificación de los RIM en las afirmaciones se debe realizar antes de considerar cualquier control relacionado, es decir, en primer lugar se debe identificar el riesgo inherente y se basa en la consideración preliminar del auditor de las incorrecciones que tienen una **probabilidad razonable** tanto de **existir** como de **ser materiales** en caso de que existan. Por eso, en esta etapa inicial, cuando se habla de RIM debe entenderse riesgos inherentes ya que es un momento previo al conocimiento y valoración de los riesgos de control, el otro componente de los RIM.

5.3 Las afirmaciones y su utilización

El auditor utiliza las afirmaciones para considerar los distintos tipos de incorrecciones potenciales que pueden existir al identificar, valorar y responder a los riesgos de incorrección material.

El apartado A-190 de la NIA-ES 315R describe y clasifica las categorías de afirmaciones tal y como aparece en el cuadro siguiente:

TTSCIR	Afirmación	Descripción
Afirmaciones sobre tipos de transacciones y hechos y la correspondiente información a revelar, durante el periodo	**Ocurrencia**	Las transacciones y hechos registrados o revelados han ocurrido y dichas transacciones y hechos corresponden a la entidad.
	Completitud	Se han registrado todos los hechos y transacciones que tenían que registrarse y se ha incluido toda la información a revelar relacionada que se tenía que incluir en los estados financieros
	Exactitud	Las cantidades y otros datos relativos a las transacciones y hechos se han registrado adecuadamente y la correspondiente información a revelar ha sido adecuadamente medida y descrita.
	Corte de operaciones	Las transacciones y los hechos se han registrado en el periodo correcto.
	Clasificación	Las transacciones y los hechos se han registrado en las cuentas apropiadas.
	Presentación	Las transacciones y hechos han sido adecuadamente agregados o desagregados y están descritos con claridad y la correspondiente información a revelar es pertinente y comprensible en el contexto de los requerimientos del marco de información financiera aplicable.
	Legalidad	Se ha cumplido la legalidad vigente en la gestión de los gastos e ingresos públicos.
Afirmaciones sobre saldos contables, y la correspondiente información a revelar, al cierre del periodo	**Existencia**	Los activos, pasivos y el patrimonio neto existen.
	Derechos y obligaciones	La entidad posee o controla los derechos de los activos, y los pasivos son obligaciones de la entidad.
	Completitud	Se han registrado todos los activos, pasivos y patrimonio neto que tenían que registrarse y se ha incluido toda la información a revelar relacionada que se tenía que incluir en los estados financieros.
	Exactitud, valoración e imputación	Los activos, pasivos y el patrimonio neto figuran en los estados financieros por los importes adecuados y cualquier ajuste resultante a la valoración o imputación ha sido adecuadamente registrado, y la correspondiente información a revelar ha sido adecuadamente medida y descrita.
	Clasificación	Los activos, pasivos y el patrimonio neto se han registrado en las cuentas apropiadas.
	Presentación	Los activos, pasivos y el patrimonio neto han sido adecuadamente agregados o desagregados y están descritos con claridad y la correspondiente información a revelar es pertinente y comprensible en el contexto de los requerimientos del marco de información financiera aplicable.

Figura 5

El auditor debe hacer preguntas relacionadas con las cantidades y revelaciones de las cuentas anuales, con el fin de identificar las afirmaciones significativas que, si no se controlan, podrían resultar en una incorrección contenida en las cuentas anuales.

***Por ejemplo**, el auditor haría preguntas tales como:*

- *¿El activo existe? (Existencia)*
- *¿Están registrados todos los ingresos? (Completitud)*
- *¿El inventario está adecuadamente valorado? (Valoración)*
- *¿Las cuentas a pagar son obligaciones propias de la entidad? (Derechos y obligaciones/Exactitud)*
- *¿Ocurrió la transacción? (Ocurrencia)*
- *¿Las cantidades están adecuadamente presentadas y reveladas en las cuentas anuales? (Clasificación/Presentación)*
- *¿cómo asegura la gerencia que las transacciones están registradas (completitud) o que las estimaciones significativas se basan en supuestos razonables y adecuadamente registrados en las cuentas anuales (exactitud y valoración)?*

5.4 Determinar las afirmaciones relevantes y los TTSCIR significativos

El auditor determinará las afirmaciones relevantes y los correspondientes TTSCIR significativos (TTSCIRS).

Las **afirmaciones relevantes** tienen por objeto centrar a los auditores en esas afirmaciones para un TTSCIR, en las que existe una **probabilidad razonable** de que se produzca una incorrección o incorrecciones y que sean materiales si se produjeran.

Es decir, **las afirmaciones relevantes son aquellas para las que el auditor ha identificado un RIM** y, por definición, **un TTSCIRS es aquel en el que hay una o más afirmaciones relevantes**.

Determinar los TTSCIR que son significativos ayuda a aclarar el trabajo del auditor en relación con el conocimiento del sistema de información, así como el desarrollo de las respuestas que son requeridas por la NIA-ES-SP 1330. Con respecto a la información a revelar, el material de aplicación en el párrafo A204 de la NIA-ES 315R explica los asuntos que pueden hacer que la información a revelar sea significativa.

La determinación de las afirmaciones relevantes y de los TTSCIRS **proporciona la base para determinar el alcance del conocimiento del sistema de información** de la entidad que el auditor debe obtener de conformidad con el apartado 25(a) de la norma. Esto es así ya que **la determinación de los TTSCIRS permite a su vez la identificación de las aplicaciones TI significativas (las que procesan esos TTSCIRS) y el entorno TI relacionado**, tal como se señala en el apartado 6.2 siguiente.

El auditor centrará su esfuerzo en aquellas áreas en las que existe un RIM/afirmación relevante/TTSCIRS.

5.5 Valoración del riesgo inherente en las afirmaciones *(párrafo 31 y32 de la GPF-OCEX 1315R)*

Para los riesgos identificados en las afirmaciones, el auditor valorará el riesgo inherente estimando la probabilidad de su ocurrencia y la magnitud de la incorrección potencial. Al hacerlo, el auditor tendrá en cuenta modo y el grado en que:

a) los FRI afectan a la susceptibilidad de las afirmaciones relevantes a incorrección; y

b) los RIM en los estados financieros afectan a la valoración del riesgo inherente en las afirmaciones.

Figura 6

Valorar el riesgo inherente implica, para cada TTSCIR, completar una tabla como la siguiente señalando todos los riesgos inherentes para las afirmaciones identificados, la probabilidad de ocurrencia y la magnitud de su impacto.

TTSCIR	Afirmación	Descripción del riesgo inherente	Probabilidad	Magnitud	Valoración
Para cada tipo de transacción	Ocurrencia				
	Completitud				
	Exactitud				
	Corte de operaciones				
	Clasificación				
	Presentación				
	Legalidad				
Para cada saldo contable	Existencia				
	Derechos y obligaciones				
	Completitud				
	Exactitud, valoración e imputación				
	Clasificación				
	Presentación				

Figura 7

La NIA-ES 315R ya no permite la posibilidad de valorar conjuntamente el riesgo inherente y el riesgo de control, **deben valorarse por separado**.

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

Dado que solo se deben tener en cuenta los riesgos materiales, para completar esta tabla se podrán descartar aquellos riesgos inherentes cuya magnitud no se acerque al nivel que previamente hayamos definido de acuerdo con las NIA-ES-SP 1320 y GPF-OCEX 1321 como incorrección claramente insignificante.

5.6 El espectro de riesgo inherente y los riesgos significativos *(párrafo 49 de la GPF-OCEX 1316R)*

El espectro de riesgo inherente es un **nuevo concepto**, muy importante, que sirve para ayudar al auditor a aplicar su **juicio profesional** al determinar la significatividad de un riesgo **combinando la probabilidad de que exista una incorrección** (considerando los factores de riesgo inherente) **y de su magnitud**.

El riesgo inherente valorado para un determinado riesgo en las afirmaciones supone haber realizado un juicio dentro de un rango, de mayor a menor, en el espectro de riesgo inherente, que puede variar según la naturaleza, dimensión y complejidad de la entidad y tiene en cuenta la valoración de la probabilidad de que ocurra una incorrección y de su magnitud, así como de los factores de riesgo inherente *(Apartado 209 de la NIA-ES 315R)*.

Cuanto mayor sea la combinación de la probabilidad de que exista y la magnitud del impacto, mayor será la valoración del riesgo inherente; cuanto menor sea la combinación de probabilidad y magnitud, menor será la valoración del riesgo inherente *(Apartados A208-209 de la NIA-ES 315R)*.

El grado en que varía el riesgo inherente es el espectro del riesgo inherente.

Para visualizarlo se puede utilizar, por ejemplo, un gráfico como el siguiente, en el que los ejes representan la probabilidad de ocurrencia en un rango de 0 a 10 y la magnitud potencial de la incorrección también en un rango de o a 10 (proporcional al nivel de importancia relativa).

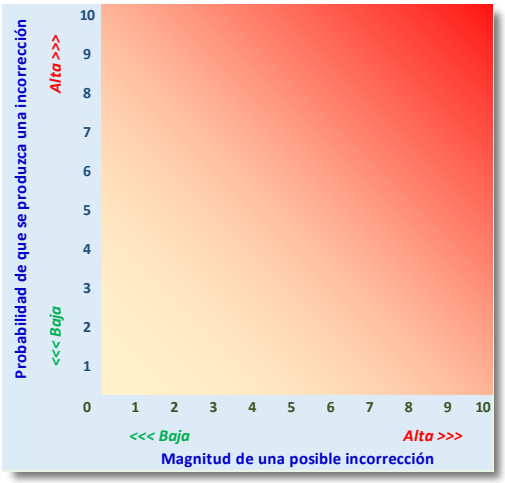

Figura 8

La intersección de la magnitud y la probabilidad determinará si el riesgo valorado es mayor o menor en el espectro de riesgo inherente. También puede representarse linealmente:

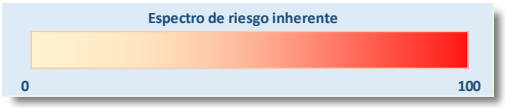

Figura 9

La valoración de los **riesgos inherentes** de esta manera ayuda a desarrollar una respuesta adecuada a los RIM.

Cuanto más alta sea la ubicación dentro del espectro de riesgo inherente del riesgo identificado, más persuasiva deberá ser la evidencia de auditoría para responder al riesgo valorado.

La norma no especifica categorizaciones a lo largo del espectro del riesgo inherente, pero sí reconoce que estas pueden ser utilizadas por los auditores.

Por razones prácticas puede resultar conveniente realizar esta categorización estableciendo tres niveles de riesgo: **A**lto, **M**oderado o **B**ajo. Esta clasificación es la que se está utilizando en distintas GPF-OCEX, aunque puede sustituirse por otra que sea más detallada. Un riesgo inherente **A**lto correspondería a un riesgo significativo, tal como se define más adelante (riesgo alto=riesgo significativo).

El auditor determinará si alguno de los riesgos valorados es un riesgo significativo[1]. Esto permitirá al auditor **centrar más su atención en los riesgos que están en la parte más alta del espectro de riesgo inherente**, realizando determinadas respuestas a esos riesgos requeridas por las NIA-ES *(Apartado 218 a 221 de la NIA-ES 315R)*.

Un **riesgo significativo** es un riesgo identificado de incorrección material para el que:

a) La valoración del riesgo inherente se encuentra próxima al **límite superior del espectro de riesgo inherente**; o

b) Debe ser tratado como riesgo significativo de conformidad con los requerimientos de otras NIA-ES (por ejemplo, riesgos de fraude).

Encontrarse próximo al límite superior en el espectro de riesgo inherente será distinto según la entidad y no significará necesariamente lo mismo para una entidad de un periodo a otro. Puede depender de la naturaleza y las circunstancias de la entidad para la que se está valorando el riesgo. Será una cuestión de juicio profesional. El párrafo A221 de GPF-OCEX 1315R ofrece algunos ejemplos de cuestiones en las que los riesgos significativos pueden ser más frecuentes.

[1] Apartado 32 de la NIA-ES 315R.

Podemos visualizarlo con un ejemplo: en una auditoría se han identificado cinco riesgos (**R**) en las afirmaciones y tras analizar los factores de riesgo inherente y otras circunstancias se ha estimado su probabilidad de ocurrencia en un rango de 0 a 10 y la magnitud potencial de la incorrección también en un rango de o a 10 (proporcional al nivel de importancia relativa). Se determinará que aquellos riesgos cuyo producto (probabilidad) por (magnitud) sea superior a un determinado nivel (60, por ejemplo) se considerarán riesgos significativos.

El rango de variación de este producto es el espectro de riesgo inherente, será:

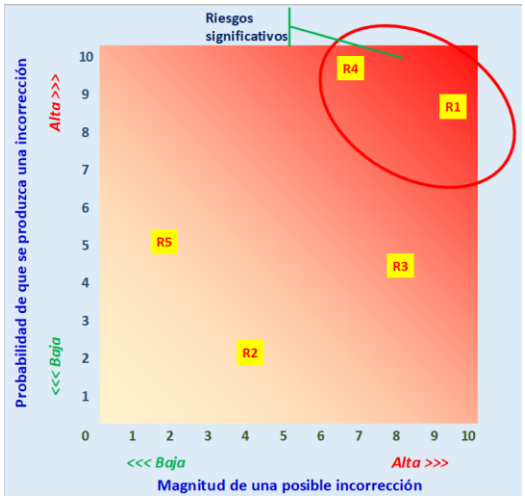

Figura 10

O en una gráfica lineal:

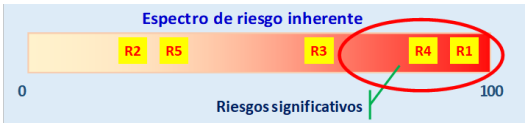

Figura 11

5.7 Riesgos para los que los procedimientos sustantivos por sí solos no proporcionan evidencia de auditoría suficiente y adecuada *(párrafo 33, A222 y A223 de la NIA-ES 315R)*

El auditor determinará si los procedimientos sustantivos por sí solos no pueden proporcionar evidencia de auditoría suficiente y adecuada con respecto a alguno de los riesgos inherentes en las afirmaciones, que han sido valorados como de incorrección material.

Debido a la naturaleza de un RIM y a las actividades de control que tratan ese riesgo, en algunas circunstancias, la única forma de obtener evidencia de auditoría suficiente y adecuada es comprobar la eficacia operativa de los controles. En consecuencia, se requiere que el auditor identifique cualquier riesgo de ese tipo por las implicaciones para el diseño y aplicación de procedimientos posteriores de auditoría de conformidad con la NIA-ES-SP 1330 para responder a los RIM en las afirmaciones.

Cuando transacciones rutinarias estén sujetas a un **procesamiento muy automatizado** con escasa o nula intervención manual, puede que **no resulte posible** aplicar únicamente procedimientos sustantivos en relación con el riesgo. Este puede ser el caso en aquellas circunstancias en las que una cantidad significativa de la información de la entidad se inicia, registra, procesa o notifica solo de manera electrónica, como en un ERP que implica un alto grado de integración a través de sus aplicaciones de TI.

En estos casos, es posible que **la evidencia de auditoría únicamente esté disponible en formato electrónico**, y que su suficiencia y adecuación normalmente dependan de la eficacia de los controles sobre su exactitud y completitud. La posibilidad de que la información se inicie o altere de manera incorrecta y de que este hecho no se detecte puede ser mayor si los correspondientes controles no están funcionando de manera eficaz.

> ***Por ejemplo**: al auditar el IBI de un gran ayuntamiento, con cientos miles de transacciones automatizadas, probablemente basarse únicamente en procedimientos sustantivos no permitirá reducir el riesgo de auditoría a un nivel aceptable y será preciso valorar el riesgo de control y revisar los CPI y los CGTI relacionados. Idéntica problemática se planteará en una entidad con decenas de miles de trabajadores en relación con la auditoría de la nómina.*

5.8 Procedimientos sustantivos que responden a riesgos significativos

La NIA-ES-SP 1330 establece en su requerimiento 21 que, si el auditor ha determinado que un riesgo valorado de incorrección material en las afirmaciones es un riesgo significativo, aplicará los procedimientos sustantivos que respondan de forma específica a dicho riesgo. Es decir, aunque las pruebas de controles son necesarias (ver apartado anterior) será preciso realizar alguna prueba sustantiva (procedimiento analítico o prueba en detalle o ambas).

Cuando la forma de enfocar un riesgo significativo consista únicamente en procedimientos sustantivos, dichos procedimientos incluirán pruebas de detalle.

5.9 Reunión del equipo para discutir sobre los riesgos *(Apartados 17 y 18; A42 y A43 de la NIA-ES 315R)*

En las etapas iniciales de la planificación debe celebrarse una reunión del auditor responsable del trabajo con el equipo de auditoría. Si ha habido rotación del equipo, también participará el auditor responsable de la fiscalización anterior.

Para cada RIM que se identifique en la reunión, el auditor describirá "qué puede ir mal". Cuanto más específica sea la respuesta a "qué puede ir mal", más sencillo será valorar el riesgo y responder al mismo. Por ejemplo, en lugar de señalar "Los gestores pueden manipular estimaciones significativas" como un riesgo, será más útil señalar que "Los gestores pueden manipular los resultados mediante cálculos que subestiman las subvenciones imputables al periodo".

Se comentará también la posible existencia de controles que mitiguen los riesgos identificados, que requerirán ser revisados en la auditoría.

Se debe estar atento a los factores de riesgo inherentes, que pueden requerir una adaptación de los procedimientos de auditoría. Cada RIM requiere su consideración de auditoría.

Esta discusión:

- Proporciona una oportunidad a los miembros del equipo con más experiencia para compartir información basada en su conocimiento de la entidad, lo que contribuye a mejorar el conocimiento de todos los miembros del equipo.
- Permite a los auditores intercambiar información sobre los riesgos de negocio a los que está sometida la entidad, sobre el modo en que los factores de riesgo inherente pueden afectar a la susceptibilidad de incorrección de los TTSCIR, así como sobre el modo en que los estados financieros de la entidad pueden ser susceptibles de incorrección material debida a fraude o error y sobre su posible localización.
- Ayuda a los miembros del equipo en la obtención de un mejor conocimiento de la posibilidad de que los estados financieros contengan una incorrección material en el área específica que les ha sido asignada, así como la comprensión de la manera en que los resultados de los procedimientos de auditoría aplicados por ellos pueden afectar a otros aspectos de la auditoría, incluidas las decisiones sobre la naturaleza, el momento de realización y la extensión de procedimientos posteriores de auditoría. En especial, la discusión ayuda a los miembros del equipo a considerar en mayor medida información contradictoria basada en el conocimiento de cada uno de los miembros acerca de la naturaleza y las circunstancias de la entidad.
- Proporciona una base para que los miembros del equipo se comuniquen y compartan nueva información, obtenida en el curso de la auditoría, que puede afectar a la valoración del RIM o a los procedimientos de auditoría realizados para responder a dichos riesgos.

La NIA-ES-SP 1240 requiere que la discusión por el equipo ponga un énfasis especial en el modo en que los estados financieros de la entidad pueden ser susceptibles de incorrección material debida a fraude y las partidas a las que puede afectar, incluida la forma en que podría producirse el fraude. (apartado 16 NIA-ES-SP 1240)

El escepticismo profesional es necesario para la evaluación crítica de la evidencia de auditoría y una discusión por el equipo del encargo sólida y abierta puede conducir a una mejor identificación y valoración de los RIM. Otro resultado de la discusión puede ser que el auditor identifique áreas específicas de la auditoría para las que puede ser especialmente importante aplicar el escepticismo profesional y puede llevar a la participación de miembros del equipo del encargo con mayor experiencia y la cualificación adecuada para participar en la aplicación de procedimientos de auditoría relacionados con esas áreas.

Esta reunión se debe documentar en los papeles de trabajo pudiendo utilizar el modelo de la ***GPF-OCEX 1513 Cómo realizar y documentar la reunión del equipo de auditoría para discutir sobre los RIM***.

6. Identificación de las aplicaciones TI significativas

Ya hemos visto que **la determinación de cuáles son los TTSCIRS permite identificar las aplicaciones TI significativas, que son aquellas que procesan esos TTSCIRS,** y el **entorno TI relacionado**.

Figura 12

En una auditoría realizada con el enfoque de riesgo, de acuerdo con las NIA-ES-SP, la identificación y conocimiento de las aplicaciones TI significativas es muy importante para la etapa de conocimiento de los riesgos inherentes y de control, y de los CPI.

El auditor obtendrá conocimiento del sistema de información y comunicación de la entidad que sea relevante para la preparación de los estados financieros, mediante la aplicación de procedimientos de valoración del riesgo a través del conocimiento de las actividades de procesamiento de la información de la entidad, incluidos sus datos e información, los recursos que se deben utilizar en esas actividades y las políticas que definen, para cada tipo de transacción, saldo contable e información a revelar significativa (TTSCIRS).

Para cada TTSCIRS este conocimiento incluirá:

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

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

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

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

(d) **los recursos de la entidad, incluido el entorno de TI**, relevantes para los apartados (a) a (c) anteriores;

En términos generales, el auditor **debe conocer** los siguientes aspectos de TI del sistema de información *(Apartados A140-A143 de la NIA-ES 315R/GPF-OCEX 1315R)*:

(a) **El modelo de negocio de la entidad y el modo en que integra la utilización de TI** ya que pueden proporcionar información útil sobre la naturaleza y extensión de las TI en el sistema de información.

(b) **La naturaleza y características de las aplicaciones de TI significativas, la infraestructura de TI en las que se apoyan y otros aspectos del entorno de TI**, a la vez que obtiene conocimiento del modo en que la información relativa a los TTSCIRS entra, fluye, se procesa y sale del sistema de información de la entidad.

En el anexo 1 se dan unas orientaciones sobre cómo realizar y documentar este trabajo, que se debe plasmar en un flujograma detallado (véase la *GPF-OCEX 1512 Cómo realizar mapas de procesos y flujogramas*) como el del ejemplo de gestión de ingresos tributarios de un ayuntamiento mostrado en el gráfico siguiente, complementado con una narrativa explicativa.

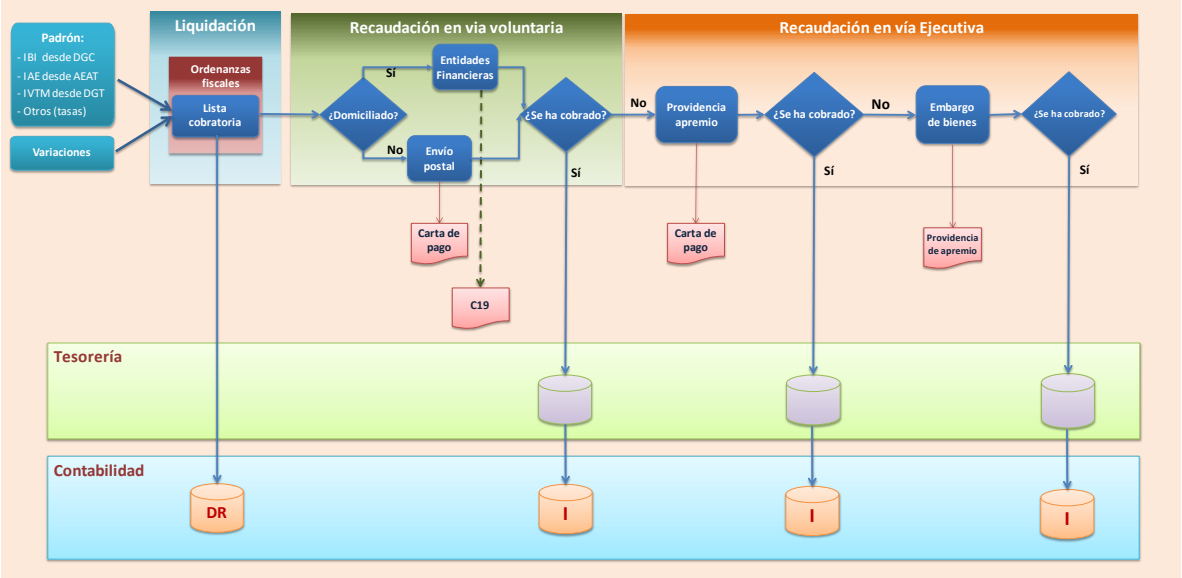

Figura 13

También identificaremos en esta fase de la auditoría las **interfaces** existentes dibujándolas como en el gráfico anterior (interfaces con Tesorería y con Contabilidad) y/o elaborando una tabla como la del siguiente ejemplo:

TTSCIRS	Aplicación TI	Interfaces
Cap 1 Ingresos por tributos	TRIBUTA	**Con contabilidad** **Con tesorería**
Cap 1 Gastos de personal	RRHH	**Con contabilidad** **Con tesorería**
Cap 2 Compras y gastos corrientes	…	**…..**

Figura 14

Por su importancia, recordaremos para facilitar la comprensión, que podemos representar el sistema de información/entorno de TI de una entidad mediante un modelo simplificado formado por varios niveles o capas tecnológicas superpuestas, tal como se muestra en la figura siguiente, en la que se distingue claramente la relación directa de los CPI con los procesos de negocio y aplicaciones de TI.

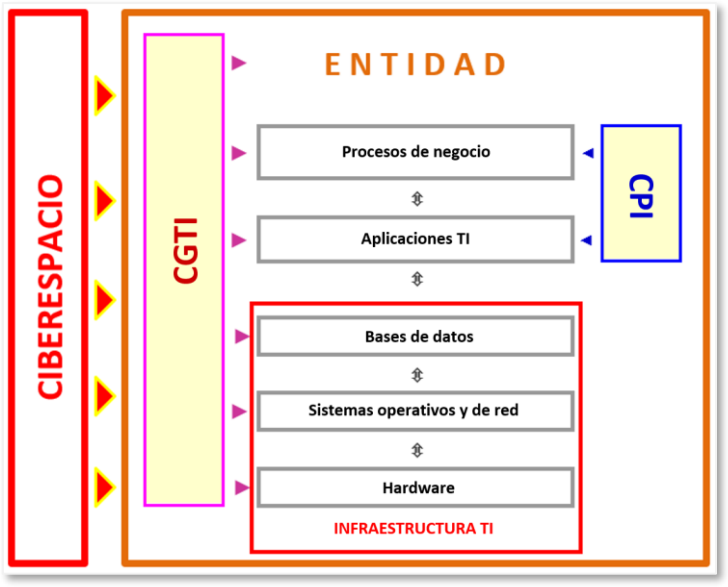

Figura 15

7 Identificación de los CPI relevantes

(apartado 26 de la NIA-ES 315R/GPF-OCEX 1315R y 32 y ss de la GPF-OCEX 1316R)

Una vez identificados los riesgos significativos y las aplicaciones TI significativas el siguiente paso será identificar los CPI relevantes y valorar el riesgo de control.

7.1 Conocimiento del componente actividades de control del sistema de control interno

Hasta ahora se exigía que el auditor identificara las **actividades de control relevantes** para la auditoría[2], **pero de forma muy general** ("*aquellas que es necesario conocer para valorar los RIM y diseñar procedimientos de auditoría posteriores que respondan a los riesgos valorados*"), sin concreción, lo que dio lugar, según la IAASB, a interpretaciones diferentes, dificultades de aplicación y prácticas incoherentes.

Figura 16

La nueva NIA-ES 315R, en el apartado 26 es muy específica, y **concreta los controles que el auditor debe conocer obligatoriamente, cuyo diseño luego debe evaluar y cuya implementación debe verificar.** El auditor deberá:

a) Identificar los controles que responden a los RIM en las afirmaciones, es decir CPI, como sigue:

i Los **controles que responden a un riesgo que se considera riesgo significativo**.

Generalmente incluyen políticas, procedimientos, prácticas y una estructura organizativa que son esenciales para que la dirección pueda reducir los riesgos y alcanzar el objetivo de control relacionado.

Incluirá el conocimiento de:

- Controles que la entidad ha diseñado e implementado para los riesgos significativos derivados de cuestiones no rutinarias o que requieran la aplicación de juicio, como por ejemplo la revisión de hipótesis por la alta dirección o por expertos, documentación de las estimaciones contables o la aprobación por los responsables de la entidad.
- Controles que la dirección ha diseñado e implementado para prevenir y detectar el fraude.

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

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

iii Los **controles cuya eficacia operativa tiene previsto comprobar el auditor** en la determinación de la naturaleza, el momento de realización y la extensión de los procedimientos sustantivos, incluyendo los **controles que responden a riesgos para los que los procedimientos sustantivos por sí solos no proporcionan evidencia de auditoría suficiente y adecuada**.

[2] Apartado 20 de la anterior NIA-ES 315.

iv **Otros controles** que el auditor considere adecuados para permitirle obtener evidencia de auditoría que permita identificar y valorar RIM y para diseñar procedimientos posteriores de auditoría que hagan frente a estos. Por ejemplo:

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

A estos controles (i a iv) los denominaremos **CPI relevantes**.

b) Identificar las aplicaciones de TI y otros aspectos del entorno de TI que están sujetos a riesgos derivados de la utilización de TI basándose en los controles identificados en el apartado a).

c) Identificar los riesgos derivados TI en las aplicaciones TI y otros aspectos del entorno TI**, y los CGTI de la entidad que responden directamente a estos riesgos**.

7.2 Los controles de procesamiento de la información (CPI)

Los CPI son controles relacionados con el procesamiento de la información en aplicaciones de TI o procesamientos manuales de la información en el sistema de información de la entidad que responden directamente a los riesgos para la integridad de la información (es decir, la completitud, exactitud y validez de las transacciones y otra información) y sobre el cumplimiento de la legalidad. Operan a nivel de procesos de gestión y se aplican al procesamiento de las transacciones mediante aplicaciones informáticas específicas.

Estos controles se extienden sobre el conjunto de un proceso de gestión o actividad soportado por una aplicación TI de gestión. **Su comprobación proporcionará confianza únicamente sobre aquellos tipos de transacciones concretos procesados por esa aplicación, ya que son controles específicos y únicos para cada aplicación TI.**

Actualmente, los procesos de gestión de los entes públicos están automatizados en gran 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 manuales tienden a desaparecer. No obstante, cuando se revisa un proceso de gestión (nóminas, compras, recaudación, etc.) se identifican todos los riesgos significativos y los controles relacionados, independientemente de si el proceso o los controles están automatizados o son manuales. Todos los controles relevantes deben revisarse, sean manuales o automáticos.

Desde el punto de vista del auditor, los **objetivos generales** de los CPI son proporcionar una garantía 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.

Objetivos generales	Descripción
Completitud	Los controles de 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, conciliaciones, totalizadores e informes de excepción*.
Exactitud	Los controles de exactitud proporcionan una seguridad razonable de que: - 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.*

Objetivos generales	Descripción
Validez	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.*
Legalidad	Los controles de legalidad proporcionan una seguridad razonable de que en la gestión de las operaciones se ha cumplido con la legalidad vigente.

Figura 17

Estos objetivos generales están directamente relacionados con las afirmaciones implícitas en la información financiera según la GPF-OCEX 1315R (apartados A190, A191 y A192).

Adicionalmente, existirán los controles de **integridad**, de **confidencialidad** y de **disponibilidad**, que son CGTI (ver GPF-OCEX 5330) 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.

Por otra parte, cada CPI tendrá sus **objetivos específicos de control** ligados al proceso de gestión en el que están implantados.

Cada tipo de aplicación exige CPI 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 CPI depende de si estos objetivos han sido alcanzados.

La **finalidad de los CPI** es establecer controles específicos sobre las aplicaciones de gestión para asegurar razonablemente que todas las transacciones son autorizadas y registradas, y que son procesadas de forma completa, adecuada y oportuna, y para garantizar la exactitud de los resultados y el cumplimiento de las normas. Los CPI 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.

7.3 Identificar los CPI que responden a los RIM en las afirmaciones

Figura 18

En esta fase, el auditor identificará los **CPI**, que son controles aplicados durante el procesamiento de la información en el sistema de información de la entidad y **responden directamente a los riesgos para la integridad de la información, es decir, la completitud, exactitud y validez de las transacciones y otra información** *(apartado A148, NIA-ES 315R).* A estos objetivos, en el sector público hay que añadir el de **legalidad**.

Teniendo en cuenta la complejidad de los procesos y de las aplicaciones de gestión en los actuales entornos de administración electrónica, es importante centrarse en lo esencial, por ello la identificación de los riesgos significativos y de los CPI implantados para mitigarlos constituye la base para una auditoría eficaz. La

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

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

Además de identificar los riesgos inherentes del proceso de gestión, en las interfaces, en los parámetros y en los datos maestros, debe adquirirse una comprensión preliminar de los CPI (manuales o automatizados) que mitiguen dichos riesgos. Solo se revisarán aquellos CPI que tengan relevancia a efectos de la auditoría, circunstancia que deberá ser definida por el auditor a partir de los riesgos significativos identificados.

Algunos tipos de CPI incluyen autorizaciones y aprobaciones, conciliaciones, verificaciones, segregación de funciones y controles físicos o lógicos, incluidos los que tratan la salvaguarda de activos. Pueden incluir controles establecidos por la dirección que responden a riesgos relacionados con información a revelar que no se haya preparado de conformidad con el marco de información financiera aplicable. Estos controles pueden estar relacionados con información incluida en los estados financieros obtenida fuera del mayor y de los auxiliares. Ver Anexo 1, apartado 3.

En la revisión de estos controles se analizará si respaldan más de un objetivo de control y si hacen frente directamente a los riesgos significativos. Cuando múltiples controles alcancen individualmente el mismo objetivo, no es necesario identificar cada uno de los controles relacionados con dicho objetivo.

Los controles automatizados pueden resultar **más fiables** que los manuales debido a que no pueden ser fácilmente evitados, ignorados o forzados y también a que están menos expuestos a simples errores. Los controles automatizados pueden ser **más eficaces** que los manuales en aquellas circunstancias en las que se produce un número elevado de transacciones recurrentes.

También conviene señalar que los CPI pueden ser de cuatros tipos: preventivos, detectivos, compensatorios y correctivos (ver figura 8 de GPF-OCEX 5330).

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

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 en ellos, la auditoría corre el riesgo de ser demasiado general e ineficaz.

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

Para documentar la valoración del riesgo de control se puede cumplimentar una tabla como la siguiente relacionando riesgos inherentes significativos para las afirmaciones[3] identificados con los CPI relevantes.

[3] Sobre las afirmaciones y su utilización ver el párrafo 44 de la GPF-OCEX 1316R.

TTSCIR	Afirmación	Riesgos (inherentes) significativos	CPI identificados
Para cada tipo de transacción	Ocurrencia		
	Completitud		
	Exactitud		
	Corte de operaciones		
	Clasificación		
	Presentación		
	Legalidad		
Para cada saldo contable	Existencia		
	Derechos y obligaciones		
	Completitud		
	Exactitud, valoración e imputación		
	Clasificación		
	Presentación		

Figura 19

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

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

(Apartado 26.d, A175 y 176 de NIA-ES 315R/GPF-OCEX 1315R y 40 de la GPF-OCEX 1316R)

Para cada uno de los controles (CPI+CGTI) identificados **que sean relevantes o significativos** el auditor debe:

a) **Evaluar si el control está diseñado (D) eficazmente** para responder al RIM en las afirmaciones (CPI) o si está diseñado eficazmente para sustentar el funcionamiento de otros controles (CGTI). Implica que el auditor considere si el control, de manera individual o en combinación con otros controles, es capaz de prevenir de modo eficaz, o de detectar y corregir, incorrecciones materiales (es decir, permite alcanzar el objetivo de control) o si es capaz de sustentar el funcionamiento de otros controles.

b) **Determinar si el control ha sido implementado (I)** estableciendo que el control existe y que la entidad lo está utilizando.

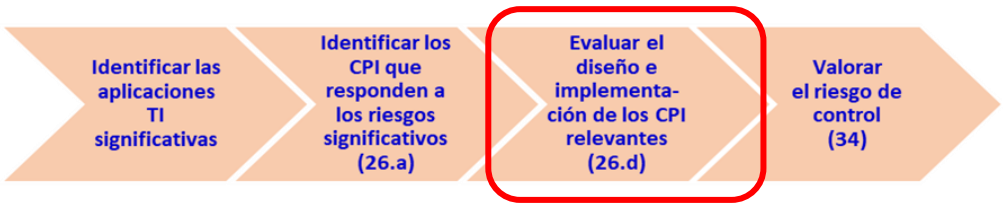

Figura 20

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

No tiene mucho sentido que el auditor evalúe la implementación de un control que no tenga un diseño eficaz. En consecuencia, el auditor evalúa en primer lugar el diseño del control, ya que un control incorrectamente diseñado o implementado puede representar una **deficiencia de control**.

Cuando el auditor haya comprobado el D+I de un CPI y vaya a confiar en su eficacia operativa como parte de su respuesta para abordar los RIM valorados y esos controles dependan de los CGTI, el auditor deberá comprobar previamente el D+I de esos CGTI y después probar la eficacia operativa de los CGTI. Ver apartado 11 siguiente.

Solo una comprensión profunda del D+I de los controles permite definir un procedimiento adecuado para evaluar su funcionamiento operativo mediante la ejecución de pruebas de cumplimiento que sean eficaces, plenamente adaptadas a la actividad 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 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 (ver apartado 12).

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 CPI, 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?
- ¿Quedan registros del funcionamiento del control para comprobaciones posteriores (logs)?

El auditor formará su opinión sobre el **diseño** de los controles:

- Entrevistando 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 pruebas paso a paso).

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 paso a paso para analizar el D+I de los controles, se llega a la conclusión de que el

esfuerzo de auditoría a efectuar para verificar un control 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 que considera inoperantes, el sistema de control evaluado presenta entonces una laguna. Para cubrirla, debe identificar otros **controles compensatorios** y evaluar su eficacia. En este caso, el auditor debe tener presente la selección completa de controles realizada para evitar crear redundancias costosas en los procedimientos de auditoría.

En todo el proceso de conocimiento e identificación de riesgos inherentes y de CPI, en la aplicación de PVR para analizar el D+I de los CPI y CGTI, y posteriormente la revisión de su eficacia operativa, el auditor estará trabajando con evidencia electrónica y deberá tener en cuenta todos los aspectos señalados en la **GPF-OCEX 1503 La evidencia electrónica de auditoría.**

Será muy frecuente que el auditor deba utilizar **herramientas y técnicas automatizadas** para obtener, analizar y extraer conclusiones de esa evidencia electrónica En estos casos se deberá aplicar la **GPF-OCEX 5370 Guía para la realización de pruebas de datos.**

9 Valoración del riesgo de control

(Apartado 34 de NIA-ES 315R/GPF-OCEX 1315R y 52 de la GPF-OCEX 1316R)

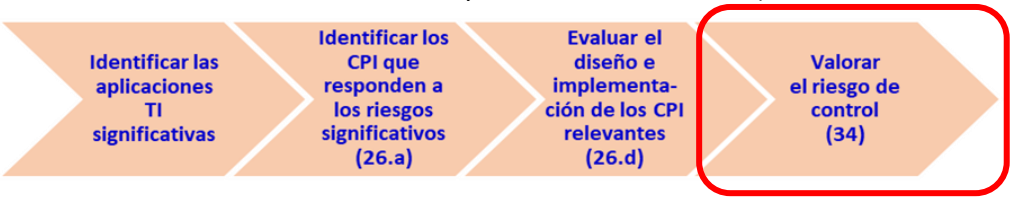

Figura 21

9.1 Valoración del riesgo

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

Si el auditor **no** tiene previsto comprobar la eficacia operativa de los controles, su valoración del RIM será la misma que la valoración del riesgo inherente[4]. En estos casos, en los que se tiene previsto adoptar un enfoque fundamentalmente sustantivo de la auditoría, una vez que se haya obtenido el conocimiento de los componentes del sistema de control interno que se exige en los apartados 21 a 27 de la NIA-ES 315R, no será necesario realizar pruebas de los controles.

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

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

9.2 Evaluación de la evidencia de auditoría obtenida de los PVR *(párrafo 35 de la NIA-ES 315R)*

El auditor evaluará si la evidencia obtenida de los PVR proporciona una base adecuada para la identificación y valoración de los RIM. En caso contrario, el auditor aplicará PVR adicionales hasta obtener evidencia de auditoría que proporcione dicha base adecuada.

En la identificación y valoración de los RIM, el auditor tendrá en cuenta toda la evidencia de auditoría obtenida de los PVR, tanto si corrobora como si contradice las afirmaciones de la dirección.

9.3 Revisión de la valoración del riesgo *(párrafo 37 de la NIA-ES 315R)*

Una vez que el auditor haya comprobado la eficacia operativa de los controles de conformidad con la NIA-ES-SP

[4] Apartado 34 de la NIA-ES 315R.

1330, podrá confirmar su expectativa inicial acerca de la eficacia operativa de los controles. Si los controles no están funcionando eficazmente según lo esperado, el auditor tendrá que revisar la valoración del riesgo de control de conformidad con el apartado 37 de la NIA-ES 315R.

Si a lo largo de la auditoría el auditor obtiene nueva información que es incongruente con la evidencia de auditoría sobre la que el auditor basó inicialmente la identificación o las valoraciones de los riesgos de incorrección material, el auditor revisará la identificación o la valoración.

10 Revisión de los CGTI

Si el auditor planea probar la eficacia operativa de un control de procesamiento de la información (CPI) automatizado, será necesario probar previamente la eficacia operativa de los CGTI relacionados que sustentan su funcionamiento continuo y eficaz. *(Apartados 26, A150 y A229 de la NIA-ES 315R)*

La NIA-ES 330 *(10.b)* 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**: 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.*

10.1 Identificar riesgos derivados del uso de las TI y los CGTI que responden a estos riesgos y revisar los CGTI

Tras la identificación de los CPI relevantes y de las aplicaciones TI significativas, el auditor debe identificar los riesgos derivados de la utilización de TI y los CGTI relacionados con dichas aplicaciones y con otros aspectos del entorno TI.

Un entorno TI está formado por las **aplicaciones de TI** y la **infraestructura que da soporte a las TI**, así como los **procesos** y **el personal** involucrado en esos procesos que una entidad utiliza para respaldar sus operaciones. Ver la figura 15 y, para más detalle, el apartado 5 de la GPF-OCEX 5330.

Todo el proceso de revisión de los CGTI está descrito con detalle en la GPF-OCEX 5330, que se sintetiza en la siguiente figura.

Figura 22

10.2 Interrelación de los CPI con los CGTI

Por regla general los CPI automatizados en aplicaciones TI son **controles directos**, que abordan los riesgos inherentes relevantes existentes en las afirmaciones, pero son **controles dependientes** del buen funcionamiento de los CGTI. Por tanto, si se va a confiar en el sistema de control interno y en los CPI es necesario identificar los riesgos derivados del uso de las TI y los CGTI que responden a estos riesgos para después revisar los CGTI y concluir sobre si aportan garantías de que los CPI tienen las condiciones adecuadas para su buen funcionamiento.

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 CPI. Sin unos CGTI efectivos, los CPI pueden dejar de ser efectivos ya que resultará mucho más fácil eludirlos.

Una evaluación favorable de los CGTI da confianza al auditor sobre los CPI 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 procesamiento de la información 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 CPI funcionen correctamente y pueden 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 CPI, es decir, comprobando si los controles de procesamiento de la información 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*.

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

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 generalizado 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.*
>
> ***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.*

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

Figura 23

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

En síntesis, el auditor debe identificar los riesgos derivados de la utilización de TI y los CGTI relacionados con las aplicaciones TI significativas identificadas y con otros aspectos del entorno de TI implementados por la entidad para responder a esos riesgos ya que **su conocimiento de puede afectar a:** *(A166 NIA-ES 315R)*

- La decisión del auditor sobre si probar la eficacia operativa de los CPI para responder a los RIM identificados en los estados financieros.

  ***Ejemplo:** Cuando los CGTI no están diseñados de un modo eficaz o no están debidamente implementados para responder a los riesgos derivados de la utilización de TI (por ejemplo, los controles no previenen o detectan cambios no autorizados en los programas o accesos no autorizados a aplicaciones de TI), esto puede influir en la decisión del auditor para no confiar en controles automatizados en la aplicación de TI afectada.*

- La valoración por el auditor del riesgo inherente en las afirmaciones.

  ***Ejemplo**: Cuando hay cambios significativos y extensos en los programas de una aplicación de TI para tratar nuevos requerimientos de información financiera, puede ser un indicio de la complejidad de estos y de su efecto en los estados financieros de la entidad. Cuando se producen tales cambios en los programas o en los datos, es probable que la aplicación de TI esté sujeta a riesgos derivados de la utilización de TI.*

- La valoración por el auditor del riesgo de control en las afirmaciones.

  ***Ejemplo:** La continuidad de la eficacia operativa de un CPI puede depender de determinados CGTI que previenen o detectan cambios no autorizados en la aplicación TI (es decir, controles sobre cambios en los programas de la aplicación*

de TI). En tales circunstancias, la esperada eficacia operativa del CGTI (o su ausencia) puede influir en la valoración por el auditor del riesgo de control (por ejemplo, el riesgo de control puede ser más elevado cuando se espera que dichos CGTI sean ineficaces o si el auditor no tiene previsto probar los CGTI).

- La estrategia del auditor para probar la información producida por la entidad generada por las aplicaciones de TI de la entidad o que involucra información originada por las mismas.

  ***Ejemplo:** Cuando la información producida por la entidad que vaya a ser utilizada como evidencia de auditoría sea generada por aplicaciones de TI, el auditor puede determinar probar controles sobre informes generados por el sistema, incluida la identificación y comprobación de los CGTI que responden a los riesgos de cambios inapropiados o no autorizados en los programas o cambios directos de datos en los informes.*

- El diseño de procedimientos posteriores de auditoría.

Por tanto, debido a la interrelación existente entre los CPI y los CGTI y a la dependencia de los primeros respecto de los segundos, que acabamos de ver, 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 procesamiento de la información 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 en el gráfico siguiente.

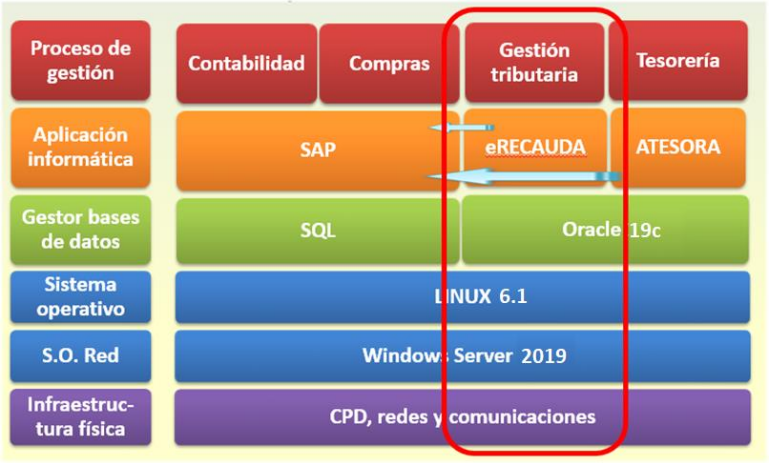

Figura 24

11 Revisión de la eficacia operativa de los CPI relevantes

(Apartados 8-17 de la NIA-ES-SP 1330 y apartado 65 de la GPF-OCEX 1316R)

11.1 Pruebas de controles

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

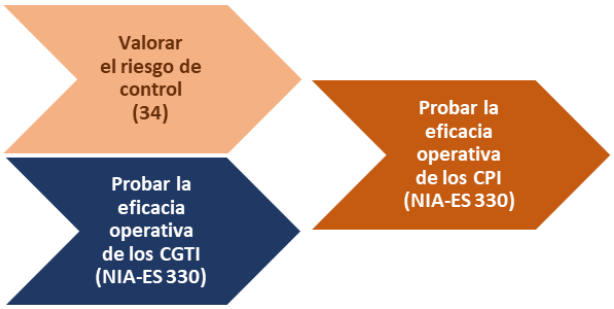

Figura 25

Sobre la eficacia operativa de los CPI relevantes la NIA-ES-SP 1330 establece lo siguiente:

8. El auditor diseñará y realizará pruebas de controles con el fin de obtener evidencia de auditoría suficiente y adecuada sobre la eficacia operativa de los controles relevantes si:

(a) la valoración de los riesgos de incorrección material en las afirmaciones realizada por el auditor comporta la expectativa de que los controles estén operando eficazmente (es decir, para la determinación de la naturaleza, momento de realización y extensión de los procedimientos sustantivos, el auditor tiene previsto confiar en la eficacia operativa de los controles); o

(b) los procedimientos sustantivos por sí mismos no pueden proporcionar evidencia de auditoría suficiente y adecuada en las afirmaciones.

9. En el diseño y aplicación de pruebas de controles, el auditor obtendrá evidencia de auditoría más convincente cuanto más confíe en la eficacia de un control.

En esta NIA-ES-SP 1330 se señalan diversos aspectos a tener en cuenta en las pruebas sobre la eficacia operativa de los controles.

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

En el caso de **CPI automatizados**, el auditor puede planificar comprobar su eficacia operativa mediante la identificación y comprobación de CGTI que aseguran el funcionamiento congruente del CPI automatizado (por ejemplo, auditando los controles de acceso y los controles de gestión de cambios) en vez de aplicar pruebas de eficacia operativa directamente sobre los CPI automatizados[5].

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

En una auditoría financiera los especialistas en auditoría de sistemas de información **analizarán con los auditores financieros** aquellos controles que son relevantes para los objetivos de la auditoría financiera, ya que no todos los riesgos son iguales, ni en probabilidad, ni en su materialidad. Se deberá adoptar un enfoque de riesgo.

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

Por otra parte, aunque es posible que algunos PVR no hayan sido específicamente diseñados como pruebas de controles, pueden, no obstante, proporcionar evidencia de auditoría sobre la eficacia operativa de los controles y, consecuentemente, ser utilizados como pruebas de controles. *(NIA-ES-SP 1330, A22)*

11.2 ¿La eficacia operativa de los CPI tiene que ser probada cada año?

En determinadas circunstancias, las normas de auditoría permiten a los auditores utilizar evidencia de auditoría sobre la eficacia operativa de los controles obtenida en auditorías anteriores. Los párrafos 13 y 14 de la NIA-ES-SP 1330 describen las consideraciones, restrictivas, para que el auditor determine si es apropiado utilizar evidencia de auditoría sobre la eficacia operativa de los controles obtenida en auditorías anteriores.

Destacaremos aquí que:

(a) **Si se han producido cambios** que afectan a la continuidad de la relevancia de la evidencia de auditoría procedente de la auditoría anterior, **el auditor realizará pruebas sobre los controles en la auditoría actual.**

(b) **Si no se han producido tales cambios, el auditor probará los controles al menos en una de cada tres auditorías,** realizando pruebas sobre algunos controles en cada auditoría para evitar la posibilidad de que

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

se prueben en un solo periodo de auditoría todos los controles en los que tenga previsto confiar y no se realice prueba alguna en los dos periodos de auditoría subsiguientes.

Cuando se trate de controles sobre riesgos significativos no se confiará en el trabajo realizado en años anteriores y se deberán realizar pruebas sobre los controles en la auditoría actual *(apartados 15 y A37b de la NIA-ES-SP 1330).*

El auditor debe también considerar la eficacia de los CGTI al determinar si las pruebas de auditoría relativas a la eficacia de un CPI en particular de un período anterior pueden utilizarse en el período actual.

Por lo general, cuanto mayor sea el riesgo de incorrección material, o mayor sea la confianza en los controles, menor ha de ser, en su caso, el intervalo entre comprobaciones. Entre los factores que pueden acortar el intervalo entre pruebas de un control, o dar lugar a que no se confíe en la evidencia obtenida en auditorías anteriores, se incluyen los siguientes: *(apartado A38 de la NIA-ES-SP 1330).*

- Un entorno de control deficiente.
- Un deficiente seguimiento de los controles.
- Un elemento manual significativo en los controles relevantes.
- Cambios de personal que afecten significativamente a la aplicación del control.
- Circunstancias cambiantes que requieran modificaciones en el control.
- CGTI deficientes.

12 Evaluación de las deficiencias de control interno detectadas

Todas nuestras comprobaciones tienen por finalidad contrastar la situación real de los CPI en la entidad, mediante la revisión del diseño e implementación y de su eficacia operativa, y evaluarlos según la siguiente escala:

Evaluación	Descripción
Control efectivo	Cubre al 100% el objetivo de control y: - El procedimiento está formalizado (documentado y aprobado) y actualizado. - El resultado de las pruebas realizadas para verificar su diseño, implementación y eficacia operativa ha sido satisfactorio.
Control bastante efectivo	En líneas generales, cumple con el objetivo de control, si bien puede haber ciertos aspectos no cubiertos al 100% y: - Se sigue un procedimiento formalizado, aunque puede presentar aspectos de mejora (detalle, nivel de actualización, nivel de aprobación, etc.). - Las pruebas realizadas para verificar la implementación son satisfactorias. - Se han detectado incumplimientos en las pruebas realizadas para verificar la eficacia operativa, pero no son ni significativos ni generalizados.
Control poco efectivo	Cubre de forma muy limitada el objetivo de control y: - Se sigue un procedimiento, aunque este puede no estar formalizado. - El resultado de las pruebas de implementación y de eficacia no es satisfactorio. Cubre en líneas generales el objetivo de control, pero: - No se sigue un procedimiento claro. - Las pruebas realizadas para verificar la implementación o la eficacia operativa no son satisfactorias (se han detectado incumplimientos significativos, aunque no están generalizados).
Control no efectivo o no implantado	No cubre el objetivo de control. El diseño cubre el objetivo de control, pero el resultado de la revisión realizada pone de manifiesto que la implementación o la eficacia operativa del control no son satisfactorias (se han detectado incumplimientos significativos y generalizados).

Figura 26. Evaluación de los controles

13 TTSCIR que no son significativos, pero sí son materiales
(párrafo 36 y A233 de la NIA-ES 315R)

En el caso de TTSCIR materiales que no se han considerado significativos, el auditor evaluará si su determinación continúa siendo adecuada.

Para finalizar el proceso de identificación de riesgos, se requiere un nuevo procedimiento una vez que el auditor se acerca al final del proceso: el auditor debe evaluar la totalidad de los TTSCIR identificados, centrándose en los que **son materiales** (ya sea cuantitativa o cualitativamente) pero que **no se han identificado como significativos** (es decir, no hay RIM identificados, no hay afirmaciones relevantes).

A los efectos de la NIA-ES 315R y apartado 18 de la NIA-ES-SP 1330 *(apartado 18)*, los TTSCIR son materiales si pudiese esperarse razonablemente que, omitiendo, revelando con incorrecciones u ocultando información sobre ellos, se influiría en las decisiones económicas que los usuarios toman basándose en los estados financieros en su conjunto. Desde un punto de vista práctico, un TTSCIR es material si es igual o superior al CIREF calculado según la GPF-OCEX 1321 (2024).

En estos casos, la NIA-ES-SP 1330 requiere que, **con independencia de los riesgos valorados de incorrección material, el auditor diseñe y aplique procedimientos sustantivos para cada TTSCIR que resulte material**.

14 Importancia relativa de las deficiencias de control a efectos de la auditoría

Al evaluar las deficiencias de control interno detectadas se deben considerar la significatividad de estas. 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; P11)*

Las deficiencias de control interno se clasifican en tres niveles de importancia relativa, que vienen definidos en la GPF-OCEX 1265 (apartado 6):

- 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.

Para evaluar la importancia relativa o significatividad de las deficiencias de control interno se tendrán en consideración los criterios señalados en el apartado 8 de la **GPF-OCEX 1265**, que debe leerse con carácter previo a la presente guía y damos por reproducido.

La evaluación de importancia relativa o significatividad de las deficiencias incluye consideraciones sobre los siguientes factores de carácter general: *(GPF-OCEX 1735; P12)*

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.

Si las deficiencias de control constituyen **debilidades materiales**, el auditor, en base al trabajo de los auditores de sistemas de información, concluirá que los controles internos no son eficaces y deberá replantearse su estrategia de auditoría, 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 auditoría. Si no se ha conseguido reducir el riesgo de auditoría a un nivel aceptable, el auditor deberá considerar la inclusión de una salvedad o una conclusión, según el tipo de informe.

15 Recomendaciones

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)*

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 27

Los hallazgos de auditoría que las soportan deberán documentarse en los papeles de trabajo e incluir: *(GPF-OCEX 1735; P9)* Criterio (de auditoría), Hecho o condición, Causa, Efecto y Recomendación.
Para elaborar las recomendaciones a realizar se tendrán en consideración los criterios señalados en la **GPF-OCEX 1735**, que debe leerse con carácter previo a la presente guía que damos por conocidos.

16 Documentación del trabajo

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

La documentación debe permitir al auditor comprender cuáles es el funcionamiento del 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		Descripción	Observaciones
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 28 Ejemplo de documentación de controles

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

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 significativos y controles relacionados, como el modelo de la figura siguiente.

Formulario de Análisis de Riesgos
Entidad: Ayuntamiento de X Y Z

Proceso de negocio: *Contratación de inversiones*
Subproceso: *Adjudicación*

Cuentas relacionadas: Capítulo 2, 6 y acreedores

Aplicación informática:

Riesgo inherente	Control (CPI)	Tipo de control	Responsable	Eficacia del control	Descripción	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/ Bastante efectivo / Poco efectivo / No efectivo o no implantado	Describir, en su caso, la deficiencia observada	Bajo Medio Alto	Describir (señalar la cuenta y la afirmación 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 29

Anexo 1. Conocimiento de las aplicaciones de TI, de las interfaces y de los CPI

1. Identificación y conocimiento de las aplicaciones de TI significativas

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 los TTSCIR significativos identificados, el auditor debe identificar los procesos de gestión relacionados y las aplicaciones de TI que los soportan.

Un **proceso de gestión** (o de negocio) consiste en una serie de actividades, operaciones o funciones (manuales, semiautomáticas o automatizadas) realizadas por una entidad, que sirven para 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, tesorería, nóminas, etc.
- Procesos **de apoyo**: agrupan todas las funciones de apoyo a la explotación de los procesos operativos, como gestión de recursos humanos, mantenimiento de inventario de inmovilizado, contabilidad, etc.

Para conocerlos mejor 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

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 de gestión pueden ser representados gráficamente mediante flujogramas (véase GPF-OCEX 1512).

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 con 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 relevantes, que deberán ser identificados y documentados por el auditor.

b) Qué es una aplicación de TI significativa

Una aplicación de TI es un programa o un conjunto de programas que se utiliza para el inicio, procesamiento, registro e información de transacciones o información. Las aplicaciones de TI incluyen almacenes de datos y generadores de informes.

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

La automatización e integración de las distintas fases de los procesos de gestión y de los controles internos en un sistema de información **plantea riesgos 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 requerirán controles específicos.

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.

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:

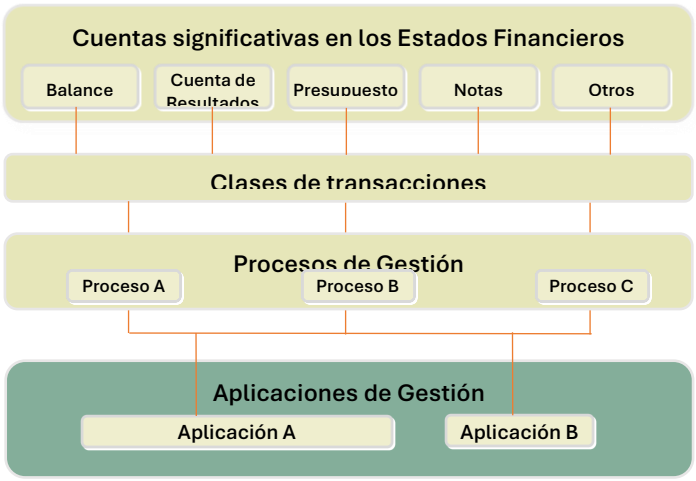

Figura 30

c) Información a obtener sobre las aplicaciones de TI y el entorno TI

El auditor basándose en:

a) la información obtenida mediante cuestionarios que se han solicitado a las entidades,
b) entrevistas mantenidas con el personal de la entidad,
c) experiencia de años precedentes,
d) el análisis de las cuentas anuales, junto con otra información obtenida en las etapas iniciales del trabajo, y
e) la identificación de los TTSCIR significativos,

determinará las aplicaciones de TI significativas, que son necesarias para la elaboración de las cuentas anuales.

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.

Será útil completar una tabla resumen con la información que se muestra la figura 31. En esta tabla se intentarán relacionar los TTSCIRS con su correspondiente proceso de gestión, con las aplicaciones de TI que lo soportan y otros datos relacionados del entorno TI.

Después de identificar las aplicaciones TI 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 se inician 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).
- 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.

d) Documentación del trabajo

El auditor debe preparar suficiente documentación, que describa claramente el proceso de gestión / aplicación de TI significativa y el entorno TI, mediante narrativas y flujogramas, y que incluya evidencia sobre la implementación de los controles.

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 TTSCIRS 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
- Identificar el entorno TI.

2. Las interfaces

a) Concepto de interfaz

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. Los entornos TI complejos generalmente requieren interfaces complejas para integrar sus aplicaciones de TI significativas.

Se deben conocer los flujos de información y de datos entre distintas funciones, aplicaciones o sistemas. Las interfaces entre aplicaciones y entre bases de datos requieren una atención especial, en particular las relacionadas con aquellas aplicaciones TI significativas.

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 una interfaz automática.

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.

Cada vez son más frecuentes las interfaces totalmente automatizadas.

Las interfaces siempre son unidireccionales, nunca bidireccionales.

ENTORNO TI DE: _____*Entidad*_____

FECHA: xx/xx/xx

Cuentas anuales		**Aplicaciones (1)**					**Bases de datos**		**Sistemas operativos**		**Plataforma hardware**	**Observaciones**
Epígrafe	Importe gestionado 2024 (euros)	Proceso	Aplicación utilizada	Tipo de aplicación **(2)**	Puesto y nombre de los responsables funcional/técnico	Control acceso (SO/aplicación) **(3)**	Marca y versión	Administrador	Marca y Versión	Puesto y nombre del responsable	Identificación marca. Denominación de los servidores	
Contabilidad												
Personal												
Compras-contratación												
Tributos												
Subvenciones												
Añadir si existen otras aplicaciones relevantes para la gestión económica de la entidad												

Figura 31

(1) Si alguno de estos procesos/aplicaciones es mantenido por un proveedor de servicios externo, indicarlo en el apartado de observaciones, señalando el nombre del proveedor y la fecha del contrato.

(2) Adquirida o de desarrollo propio.

(3) Entorno que ofrece el control en el acceso lógico a la aplicación: delegada en el sistema operativo (SO) u otro sistema o de la propia aplicación.

Nota: En el caso de aplicaciones que soportan procesos que se van a auditar, adjuntar el modelo de datos de la base de datos o la documentación existente sobre el modelo de datos, los manuales de usuario de la aplicación y los informes de auditoría de sistemas de información sobre la aplicación realizados en el último año. Solo se aportará la información que se disponga, no es necesario elaborar documentación ad hoc. Si no se dispone de documentación, señalarlo.

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.

El riesgo de interfaz (externas e internas) surge cuando no son adecuadamente diseñadas, implementadas, documentadas y programadas. Estos riesgos de interfaz, con frecuencia, llevan a una pérdida de integridad de los 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.

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.

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

c) Consideraciones de auditoría sobre las interfaces

Las interfaces deben describirse 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.

La revisión de las interfaces pasa por la comprensión del tipo de interfaz analizada (manual, automática, etc), para identificar los tipos de controles internos aplicados y para detectar los riesgos asociados.

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?

- ID de interfaz: 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?

Las características de las interfaces afectan a la valoración 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.

Si los métodos de revisión varían según el tipo de interfaz, el objetivo de la auditoría 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.).

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 HTA es un procedimiento que proporciona confianza sobre la integridad de la información transmitida entre distintos sistemas.

e) Documentación de las interfaces

El auditor debe obtener un conocimiento suficiente de las aplicaciones significativas e interfaces 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 32

3. Principales tipos de CPI

Los CPI son los controles automatizados y manuales aplicados en el flujo de procesamiento de las transacciones. Se refieren a la completitud, exactitud, validez y legalidad de las transacciones y datos durante su procesamiento. Operan a lo largo del proceso de gestión.

Las áreas específicas de controles de procesamiento de la información son:

a) Controles de entrada de datos
b) Controles sobre el procesamiento de los datos
c) Controles sobre la salida de los datos
d) Controles sobre los datos maestros
e) Controles sobre las interfaces
f) Segregación de funciones

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 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.
- 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.
- 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 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 completos 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 ficheros maestros contienen 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 ficheros 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

Los controles de interfaz son aquellos diseñados para el procesamiento o trasferencia 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.

f) 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.

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 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 conciliándolos con los modelos RLC y RNT (cotizaciones a la seguridad social), y los modelos 110 y 190 (declaración de retribuciones y retenciones a efectos del IRPF).
- Si un empleado que participa en la elaboración de la nómina también mantiene el fichero maestro de empleados (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, es conveniente utilizar una matriz en la 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.

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.

Anexo 2. Conocimiento de los factores de riesgo inherente (FRI)

En este anexo, basado en el ***Anexo 2 de GPF-OCEX 1315 Revisada*** se proporciona una explicación más detallada de los FRI, así como cuestiones que el auditor puede considerar para el conocimiento y aplicación de los FRI para la identificación y valoración de riesgos de incorrección material (RIM) en las afirmaciones.

Los factores de riesgo inherente

1. El conocimiento de la entidad y de su entorno y del marco de información financiera aplicable ayuda al auditor en la identificación de hechos o condiciones cuyas características pueden afectar a la susceptibilidad de las afirmaciones sobre TTSCIR a incorrección. Estas características son FRI, que pueden ser cualitativos o cuantitativos y afectar a la susceptibilidad de las afirmaciones a incorrección.
2. Los factores de riesgo inherente **cualitativos** relativos a la preparación de información requerida por el marco de información financiera aplicable incluyen:
    - complejidad;
    - subjetividad;
    - cambio;
    - incertidumbre o
    - susceptibilidad de incorrección debida a sesgo de la dirección u otros factores de riesgo de fraude en la medida en la que afecten al riesgo inherente.
3. Otros factores de riesgo inherente (**cuantitativos**), que afectan a la susceptibilidad de una afirmación sobre un tipo de transacción, saldo contable o revelación de información a incorrección pueden incluir:
    - la significatividad cuantitativa o cualitativa del TTSCIR;
    - el volumen o la falta de uniformidad en la composición de los elementos que deben ser procesados a través del tipo de transacción o saldo contable, o reflejado en la información a revelar.
4. El conocimiento del modo en que los factores de riesgo inherente afectan a la susceptibilidad de las afirmaciones a incorrección puede facilitar al auditor un conocimiento preliminar de la probabilidad o magnitud de las incorrecciones, lo que ayuda al auditor a identificar los riesgos de incorrección material en las afirmaciones de conformidad con el apartado 28(b) de la NIA-ES 315R. El conocimiento del grado en que los factores de riesgo inherente afectan a la susceptibilidad de las afirmaciones a incorrección también ayuda al auditor en la valoración de la probabilidad y la magnitud de una posible incorrección cuando valora el riesgo inherente de conformidad con el apartado 31(a) de la NIA-ES 315R.

    En consecuencia, el conocimiento de los factores de riesgo inherente también puede ayudar al auditor en el diseño y aplicación de los procedimientos posteriores de auditoría de conformidad con la NIA 330.
5. La identificación por el auditor de los riesgos de incorrección material en las afirmaciones y la valoración del riesgo inherente también pueden verse influidas por evidencia de auditoría obtenida en la aplicación de otros procedimientos de valoración del riesgo, de procedimientos posteriores de auditoría o en el cumplimiento de otros requerimientos de las NIA.
6. El grado de susceptibilidad de incorrección de un TTSCIR originada por la **complejidad o la subjetividad**, a menudo, está estrechamente vinculado al grado en el que está sujeto a **cambios o incertidumbre**.

    Cuanto mayor sea el grado de susceptibilidad de incorrección material de un TTSCIR debida a **complejidad o subjetividad**, mayor será la necesidad del auditor de aplicar **escepticismo profesional**.

    Además, cuando un TTSCIR es susceptible de incorrección debido a complejidad, subjetividad, cambio o incertidumbre, estos FRI pueden crear oportunidades para el sesgo de la dirección, intencionado o no, y afectar a la susceptibilidad de incorrección debida a sesgo de la dirección. La identificación por el auditor de los RIM y la valoración del riesgo inherente en las afirmaciones también pueden verse afectadas por las interrelaciones entre los FRI.

7. Algunos de los FRI relativos a la preparación de información requerida por el marco de información financiera aplicable (denominados en este apartado "información requerida") incluyen los aspectos señalados en los siguientes apartados.

También figuran ejemplos de hechos (incluidas transacciones) y de condiciones que pueden indicar la existencia de RIM en los estados financieros o en las afirmaciones. Estos ejemplos abarcan un amplio espectro de hechos y condiciones; sin embargo, no todos son relevantes para todas las auditorías y la lista de ejemplos no es exhaustiva. Es importante tener en cuenta que, debido a las interrelaciones entre los FRI, los hechos y las condiciones de los ejemplos también pueden estar sujetos a otros FRI en distinto grado o ser afectados por ellos.

8. Complejidad

Se origina, bien por la naturaleza de la información, bien por el modo en que se prepara la información requerida, incluido cuando dichos procesos de preparación son inherentemente más difíciles de aplicar. Por ejemplo, la complejidad puede surgir:

- en el cálculo de provisiones para descuentos de proveedores porque puede ser necesario tener en cuenta distintos términos comerciales con muchos proveedores distintos, o muchos términos contractuales interrelacionados que son, todos ellos, aplicables en el cálculo de los descuentos a abonar;
- cuando existen muchas fuentes posibles de datos, con diferentes características que se utilizan en la realización de una estimación contable, el procesamiento de esos datos implica muchos pasos interrelacionados y los datos, en consecuencia, son inherentemente más difíciles de identificar, capturar, acceder, comprender o procesar; o
- cuando el procesamiento de las transacciones se realiza de forma automatizada en un sistema de información de elevada complejidad tecnológica.

Ejemplos de hechos o condiciones que pueden indicar la existencia de RIM en las afirmaciones
Normativa: • Operaciones sujetas a un alto grado de regulación compleja. Modelo de negocio: • Existencia de alianzas y de negocios conjuntos complejos. Marco de información financiera aplicable: • Mediciones contables que conllevan procesos complejos. Transacciones: • Utilización de financiación fuera de balance, entidades con cometido especial y otros acuerdos de financiación complejos.

Cuando la complejidad es un FRI, puede existir una necesidad inherente de procesos más complejos para la preparación de la información, y esos procesos pueden ser inherentemente más difíciles de aplicar. Como resultado, su aplicación puede requerir cualificaciones o conocimientos especializados y la utilización de un experto de la dirección.

9. Subjetividad

Se origina por limitaciones inherentes en la capacidad de preparar la información requerida de un modo objetivo, debido a limitaciones en la disponibilidad de conocimiento o de información, de tal modo que la dirección puede tener que elegir o aplicar un juicio subjetivo acerca del enfoque más adecuado y acerca de la información resultante que se debe incluir en los estados financieros. Debido a distintos enfoques en la preparación de la información requerida, se podrían producir diferentes resultados de una adecuada aplicación del marco de información financiera aplicable. A medida que aumentan las limitaciones en el conocimiento o en los datos, aumenta la subjetividad de los juicios que podrían aplicar personas razonablemente conocedoras e independientes, así como la diversidad de los posibles resultados de esos juicios.

Ejemplos de hechos o condiciones que pueden indicar la existencia de RIM en las afirmaciones
Marco de información financiera aplicable: • Una amplia variedad de posibles criterios de medición de una estimación contable. Por ejemplo, el reconocimiento por la dirección de la amortización o de los ingresos y gastos de construcción. • La elección por la dirección de una técnica o modelo de valoración para un activo no corriente, como inversiones inmobiliarias.

Cuando el juicio de la dirección es más subjetivo, la susceptibilidad de incorrección debida a sesgo de la dirección, intencionado o no, también puede ser mayor. Por ejemplo, puede ser necesaria la aplicación de juicios significativos por la dirección para la realización de estimaciones contables que se han identificado como estimaciones con una elevada incertidumbre en la estimación, y las conclusiones relativas a los métodos, datos e hipótesis pueden reflejar sesgo de la dirección, intencionado o no.

10. Cambio

Es el resultado de hechos o condiciones que, a lo largo del tiempo, afectan al negocio de la entidad o a los aspectos económicos, contables, normativos, sectoriales u otros del entorno en el que opera, cuando se reflejan los efectos de esos hechos o condiciones en la información requerida. Dichos hechos o condiciones pueden ocurrir durante el periodo de información financiera o entre periodos. Por ejemplo, el cambio puede ser el resultado de desarrollos en los requerimientos del marco de información financiera aplicable, en la entidad y su modelo de negocio o en el entorno en el que opera la entidad. Dicho cambio puede afectar a las hipótesis y juicios de la dirección, incluido cuando está relacionado con la elección de políticas contables por la dirección o el modo en que se realizan las estimaciones contables o se determina la correspondiente información a revelar.

Ejemplos de hechos o condiciones que pueden indicar la existencia de RIM en las afirmaciones
Condiciones económicas: • Operaciones en regiones económicamente inestables; por ejemplo, en países con significativa devaluación de la moneda o con economías muy inflacionistas. Mercados: • Operaciones expuestas a mercados volátiles; por ejemplo, comercio con futuros. Pérdida de clientes: • Problemas de empresa en funcionamiento y de liquidez, incluida la pérdida de clientes significativos. Modelo sectorial: • Cambios en el sector en el que opera la entidad. Modelo de negocio: • Cambios en la cadena de suministros. • Desarrollo u oferta de nuevos productos o servicios, o cambios a nuevas líneas de negocio. Geografía: • Expansión a nuevas ubicaciones. Estructura de la entidad: • Cambios en la entidad, como importantes adquisiciones o reorganizaciones u otros hechos inusuales. • Probabilidades de venta de entidades o de segmentos de negocio. Competencia de los recursos humanos: • Cambios en personal clave, incluida la salida de ejecutivos clave. **TI:** • Cambios en el entorno de las TI. • Instalación de nuevos y significativos sistemas de TI relacionados con la información financiera. Marco de información financiera aplicable: • Aplicación de nuevos pronunciamientos contables. Capital: • Nuevas restricciones en la disponibilidad de capital y de créditos.

Ejemplos de hechos o condiciones que pueden indicar la existencia de RIM en las afirmaciones
Normativa: • Inicio de investigaciones sobre las operaciones de la entidad o sobre sus resultados realizadas por organismos reguladores o gubernamentales. • Impacto de nueva legislación relacionada con la protección del medioambiente.

11. Incertidumbre

Surge cuando la información requerida no se puede preparar solo sobre la base de datos suficientemente precisos y completos que se pueden verificar mediante observación directa. En estas circunstancias, es posible que se tenga que adoptar un enfoque que aplica el conocimiento disponible para preparar información utilizando datos observables suficientemente precisos y completos, siempre que estén disponibles y, cuando no lo estén, hipótesis sustentadas por los datos más adecuados de que se disponga. Las restricciones sobre la disponibilidad de conocimiento o datos, que no se encuentran bajo control de la dirección (sujetas, en su caso, a restricciones de coste) son fuentes de incertidumbre y su efecto en la preparación de la información requerida no se puede eliminar. Por ejemplo, la incertidumbre en la estimación surge cuando el importe monetario requerido no se puede determinar con precisión y el resultado de la estimación no se conoce antes de la fecha en que se finalizan los estados financieros.

Ejemplos de hechos o condiciones que pueden indicar la existencia de RIM en las afirmaciones
Preparación de información: • Hechos o transacciones que implican una incertidumbre significativa de medición, incluidas las estimaciones contables, y la correspondiente información a revelar. • Litigios y pasivos contingentes pendientes; por ejemplo, garantías post-venta, garantías financieras y reparación medioambiental.

12. Susceptibilidad de incorrección debida a sesgo de la dirección u otros factores de riesgo de fraude en la medida en la que afectan al riesgo inherente

La susceptibilidad de sesgo de la dirección es el resultado de condiciones que originan susceptibilidad de que la dirección no mantenga, intencionadamente o no, la neutralidad en la preparación de la información. El sesgo de la dirección se asocia con frecuencia a determinadas condiciones que tienen la posibilidad de dar lugar a que la dirección no mantenga la neutralidad al aplicar el juicio (indicadores de sesgo potencial de la dirección), lo que podría dar lugar a una incorrección material en la información que, si fuera intencionada, sería fraudulenta.

Dichos indicadores incluyen incentivos o presiones en la medida en que afectan al riesgo inherente (por ejemplo, como resultado de una motivación para alcanzar un determinado resultado, tal como un objetivo de beneficio o una ratio de capital) y la oportunidad de no mantener la neutralidad. En los apartados A1 a A5 de la NIA-ES-SP 240 se describen factores relevantes para la susceptibilidad de incorrección debida a fraude bajo la forma de información financiera fraudulenta o de apropiación indebida de activos.

Ejemplos de hechos o condiciones que pueden indicar la existencia de RIM en las afirmaciones
Preparación de información: • Oportunidades para que la dirección y los empleados produzcan información financiera fraudulenta, incluida la omisión o la ocultación de información significativa en la información a revelar. Transacciones: • Transacciones significativas con partes vinculadas. • Número significativo de transacciones no rutinarias o no sistemáticas, incluidas transacciones intragrupo e importantes transacciones generadoras de ingresos al cierre del periodo. • Transacciones registradas sobre la base de las intenciones de la dirección; por ejemplo, refinanciación de la deuda, activos mantenidos para la venta y clasificación de los valores negociables.

13. Otros hechos o condiciones que pueden ser indicativas de la existencia de RIM en los estados financieros

- Falta de personal con las cualificaciones necesarias en el área contable y de información financiera.
- Deficiencias de control, en particular en entorno de control, en el proceso de valoración del riesgo y en el proceso de seguimiento y, especialmente, en las no tratadas por la dirección.
- Incorrecciones anteriores, historial de errores o un elevado número de ajustes al cierre del periodo.

14. Efecto de los sistemas de información sobre el riesgo inherente[6]

Los sistemas de información no afectan a los objetivos de auditoría de un TTSCIR. Sin embargo, los sistemas de información (o la falta de ellos) pueden introducir FRI que no están presentes en un sistema de contabilidad manual.

El auditor debe (1) considerar cada uno de los siguientes aspectos del sistema de información y (2) evaluar su impacto global en el riesgo inherente. Normalmente el impacto de estos factores será **generalizado**. Un auditor de sistemas de información puede ayudar al auditor financiero o de cumplimiento a considerar estos factores y analizar su impacto.

El auditor identificará FRI basado en su comprensión de las áreas de interés de auditoría, incluida la tecnología de la información que la entidad emplea en esas áreas. La utilización de TI por la entidad puede introducir **FRI**, como los siguientes:

a) La coherencia de la **estructura de seguridad** y privacidad a nivel de sistema con la estructura organizativa de la entidad, así como las estrategias de misión y de negocio de la entidad, pueden afectar el diseño de los sistemas de información y los controles de seguridad relacionados.

b) La **complejidad de las operaciones de TI** de la entidad, incluida la medida en que agentes externos realizan operaciones de TI, incluidas las funciones de seguridad de la información y privacidad, en nombre de la entidad, puede dar lugar a un mayor riesgo inherente.

c) Procesamiento uniforme de las transacciones. Debido a que los sistemas de información procesan grupos de transacciones idénticas de manera consistente, cualquier incorrección que surja de una programación informática errónea ocurrirá consistentemente en transacciones similares. Sin embargo, la posibilidad de errores de procesamiento aleatorios se reduce sustancialmente con un procesamiento informatizado.

d) Procesamiento automático. El sistema de información puede iniciar automáticamente transacciones o realizar funciones de procesamiento. La evidencia de estos pasos de procesamiento (y cualquier control relacionado) puede o no ser visible.

e) Mayor potencial de incorrecciones no detectadas. Los ordenadores utilizan y almacenan información en forma electrónica y requieren menos participación humana en el procesamiento. Esto aumenta la posibilidad de que las personas obtengan acceso no autorizado a información confidencial y alteren los datos sin evidencia visible. Debido a su formato electrónico, los cambios en los programas de software y en los datos pueden no ser fácilmente detectables.

Además, los usuarios pueden ser menos propensos a desconfiar en la fiabilidad de los datos proporcionados por un ordenador que de los informes manuales. Así, la gerencia debe evaluar las amenazas a la seguridad, que pueden provenir de fuentes internas o externas. Las amenazas externas son particularmente importantes para las entidades que dependen de las redes de telecomunicaciones e Internet. Las amenazas internas pueden provenir de antiguos empleados o de descontentos.

f) Existencia, completitud y volumen de la pista de auditoría. La pista de auditoría es la evidencia que demuestra cómo se inició, procesó, registró y acumuló una transacción específica.

Por ejemplo, la pista de auditoría de una compra podría incluir una orden de compra, un albarán de recepción, una factura, un registro de facturas (compras resumidas por día, mes, cuenta o una combinación de estas) y asientos del libro mayor. Algunos sistemas de gestión financiera están

[6] Fuente: Sección 260.12 del Financial Audit Manual (FAM), y Sección 260.05 del Federal Information System Controls Audit Manual (FISCAM), del U.S. Government Accountability Office (GAO).

diseñados para que la pista de auditoría solo exista durante un corto período, solo en formato electrónico, o solo en forma resumida. Además, la información generada puede ser demasiado voluminosa para permitir una revisión manual efectiva. Por ejemplo, un asiento en contabilidad puede resultar de la síntesis automatizada de información de cientos o miles de documentos.

En algunos sistemas de información, las pistas de auditoría y la información de soporte que producen los sistemas pueden estar limitadas en su utilidad como base para la aplicación de determinados tipos de controles o como evidencia de auditoría.

g) Cambios en aplicaciones y en el entorno TI.

h) Naturaleza del hardware y software de los sistemas de información. La naturaleza del hardware y software de los sistemas de información puede afectar al riesgo inherente, como se ilustra a continuación.

- El tipo de procesamiento del sistema de información (en línea, orientado por lotes o distribuido) presenta diferentes niveles de riesgo inherente. Por ejemplo, el riesgo inherente de transacciones no autorizadas y errores de entrada de datos puede ser mayor para el procesamiento en línea que para el procesamiento orientado a lotes.
- Los dispositivos de acceso periférico o las interfaces del sistema pueden aumentar el riesgo inherente. Por ejemplo, el acceso a Internet y el acceso telefónico a un sistema aumentan el riesgo de acceso no autorizado a los recursos informáticos.
- Las redes distribuidas permiten que múltiples equipos TI se comuniquen entre sí, lo que aumenta el riesgo de acceso no autorizado a los recursos informáticos y la posible alteración de los datos.
- La forma en que se estructuran las redes de la entidad, así como la configuración de sus componentes, afectan las rutas de acceso entrantes y salientes de los sistemas de información relevantes. Por ejemplo, los factores que aumentan el riesgo inherente incluyen un número significativo de puntos de acceso a Internet que no están controlados de forma centralizada; redes que no estén segmentadas para proteger la información y los sistemas de información sensibles; y la falta de herramientas y software que mejoren la seguridad de la red, como los sistemas de detección y prevención de intrusiones.
- Los sistemas de información altamente descentralizados, en particular las aplicaciones web, añaden complejidad y aumentan las vulnerabilidades potenciales.
- Los aplicativos software desarrollados internamente pueden tener un riesgo inherente más alto que el software suministrado por un proveedor, que ha sido probado a fondo y es de uso comercial. Por otro lado, es posible que el software suministrado por el proveedor sea nuevo para uso comercial y no haya sido probado a fondo o sometido a pruebas por el cliente en un grado que encuentre fallos existentes.
- Ciertos tipos de hardware y software en uso pueden ser más susceptibles a amenazas que otros. Por ejemplo, el hardware o software que no está actualizado o parcheado, así como los componentes del sistema de información no soportado por el fabricante, presentan un riesgo inherente mayor que aquellos que son actualizados, parcheados y soportados por el desarrollador, proveedor o fabricante.
- El uso por la entidad de tecnología nueva o emergente puede aumentar el riesgo de que las configuraciones de seguridad de los componentes correspondientes no estén bien desarrolladas o probadas, o que el personal de TI no tenga los conocimientos, experiencia y habilidades necesarias para seleccionar e implementar adecuadamente los controles de seguridad sobre dicha tecnología.
- Debido a la naturaleza del hardware y software de los sistemas de información, la dirección debe diseñar controles para limitar el acceso de los usuarios a los sistemas de información a través de controles de acceso, que incluirán su rápida actualización cuando los empleados cambien de funciones de trabajo o abandonen la entidad.

i) **Transacciones inusuales.** Al igual que con los sistemas manuales, las transacciones inusuales del sistema de información aumentan el riesgo inherente. Los programas desarrollados para procesar tales transacciones pueden no estar sujetos a los mismos procedimientos que los programas desarrollados para procesar transacciones rutinarias.

El auditor debe identificar factores de riesgo inherentes y de control relevantes para los procesos de negocio significativos y áreas de interés de auditoría. El auditor identifica factores de riesgo inherentes y de control en el contexto de los objetivos de seguridad de la información y la relación de dichos objetivos con el logro de objetivos de procesamiento de información que son significativos para la auditoría.

El auditor identifica FRI basado en la información obtenida durante la fase de planificación para desarrollar un conocimiento de las operaciones de la entidad, los procesos de negocio significativos y los CPI, incluidas las operaciones, procesos o controles externos que se realizan en nombre de la entidad.

El auditor utiliza el juicio profesional para determinar (1) la extensión de los procedimientos de valoración del riesgo necesarios para identificar los factores de riesgo inherentes y de control y (2) el efecto de dichos factores de riesgo en la valoración preliminar del riesgo de TI por parte del auditor.

El efecto de los factores de riesgo inherentes puede ser de carácter generalizado dependiendo de la extensión con la que se utilice la misma tecnología de la información en relación con múltiples áreas de interés para la auditoría.