GPF-OCEX 1316 Guía de implementación por primera vez de la GPF-OCEX 1315 (Revisada)

Referencia: GPF-OCEX 1315 (Revisada)

Documento elaborado por la Comisión Técnica de los OCEX y
aprobado por la Conferencia de Presidentes de ASOCEX el 03/11/2022. *Actualizado el 19/10/2023.*

I. Introducción

II. Procedimientos de valoración del riesgo

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

IV. Identificación y valoración del RIM

V. La NIA-ES 315 (Revisada) y la auditoría pública en un entorno de administración electrónica avanzada

VI. Documentación

VII. Bibliografía

VIII. Acrónimos utilizados

Control de versiones

I Introducción

1. En octubre de 2021, mediante Resolución de 14 de octubre de 2021, del Instituto de Contabilidad y Auditoría de Cuentas, se publicaron las Normas Técnicas de Auditoría siguientes, resultado de la adaptación de las Normas Internacionales de Auditoría para su aplicación en España: NIA-ES 250 (Revisada) "Consideración de las disposiciones legales y reglamentarias en la auditoría de estados financieros", **NIA-ES 315 (Revisada) "Identificación y valoración del riesgo de incorrección material"** y NIA-ES 610 (Revisada) "Utilización del trabajo de los auditores internos".

   Aunque las tres NIA-ES son importantes, **las novedades que introduce la nueva NIA-ES 315 (Revisada) son especialmente relevantes por los cambios que introduce respecto de la anterior norma y por su gran impacto en la actividad de los auditores**.

   La nueva NIA-ES 315 (Revisada) o NIA-ES 315R representa un cambio muy importante respecto de la anterior, pero ese cambio va a ser más suave para los auditores de los OCEX que apliquen las Guías prácticas de fiscalización de los OCEX (GPF-OCEX) ya que gran parte de los aspectos novedosos relacionados con la metodología y tecnología ya están considerados en las GPF-OCEX y hace años que se adaptó la NIA-ES 315 para su uso en entornos de administración electrónica avanzada (AEA). Las GPF-OCEX que recogen, hasta 2022, esta metodología son:

GPF-OCEX 1315	Identificación y valoración de los riesgos de incorrección material mediante el conocimiento de la entidad y de su entorno
GPF-OCEX 1316	El conocimiento requerido del control interno de la entidad
GPF-OCEX 1317	Guía para la identificación y valoración de los Riesgos de Incorrección Material
GPF-OCEX 5330	Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica
GPF-OCEX 5340	Los controles de aplicación: qué son y cómo revisarlos

   Aunque estas guías recogen en buena medida la metodología introducida por la NIA-ES 315R resulta necesario revisarlas y alinearlas completamente con esta norma. Para ello **se derogan las tres primeras** y sustituyen por:

   a) GPF-OCEX 1315 Identificación y valoración del riesgo de incorrección material (Revisada) o GPF-OCEX 1315R.

   Esta guía recoge íntegramente la nueva NIA-ES 315R y se han modificado dos cosas importantes:

   - Se ha cambiado una incorrecta traducción del término inglés "completeness", que en la NIA-ES 315R se ha traducido por integridad, igual que "integrity", lo cual en condiciones normales no tendría mayor importancia, pero en el contexto de la NIA puede ocasionar confusión (como en las definiciones circulares

de 12.d y 12.e). Por eso en la GPF-OCEX se ha utilizado "completitud" para diferenciar de "integridad", de acuerdo con el original en inglés, distinguiendo claramente estos dos diferentes conceptos.

- También se han incorporado los apartados "Consideraciones específicas para entidades del sector público" eliminados por el ICAC para la versión NIA-ES 315R ya que está dirigida a los auditores privados.

b) GPF-OCEX 1316 Guía de implementación por primera vez de la GPF-OCEX 1315 Identificación y valoración del riesgo de incorrección material (Revisada).

La NIA-ES 315R, a pesar de las indudables mejoras introducidas para facilitar su lectura y comprensión, **sigue siendo una norma compleja y larga** (100 páginas y más de 50.000 palabras) y se necesitan ayudas para su aplicación inicial. Por esta razón, la Comisión Técnica de los OCEX (CT-OCEX) ha elaborado esta guía, que **es puramente descriptiva y no introduce ningún requerimiento obligatorio adicional**.

En esta GPF-OCEX 1316 se enumeran las principales novedades que se introducen en la NIA-ES 315R/GPF-OCEX 1315R y cuál va a ser su impacto sobre las auditorías públicas que realizan los OCEX.

Está dirigida a los auditores de los OCEX y su objetivo es ayudar a comprender los requerimientos y los principales cambios introducidos respecto de la anterior norma y de ninguna manera sustituye la lectura y conocimiento de la NIA-ES 315R/GPF-OCEX 1315R. Tampoco es una guía completa de la norma, ya que hay aspectos que no son tratados en esta guía con la profundidad y detalle necesario.

La NIA-ES 315R/GPF-OCEX 1315R debe leerse completa con carácter previo a la presente guía.

Las GPF-OCEX 5330 y GPF-OCEX 5340 son plenamente vigentes con la nueva NIA-ES 315R/GPF-OCEX 1315R, si bien próximamente deberán ser objeto de una revisión de aspectos no esenciales para alinearlas plenamente con la nueva norma y con el nuevo Esquema Nacional de Seguridad aprobado en 2022.

Aunque está pendiente de aprobarse por la IGAE la versión para el sector público, la NIA-ES-SP 1315 (Revisada), la Comisión Técnica de los OCEX considera conveniente la actualización de las GPF-OCEX en los términos arriba indicados, ya que su aplicación no representa en la práctica un cambio significativo respecto de las vigentes hasta el momento, pero se modernizan algunos aspectos esenciales para nuestra práctica ajustándose a la realidad de nuestro entorno de administración electrónica avanzada.

Cualquier comentario realizado sobre la NIA-ES 315R es también aplicable a la GPF-OCEX 1315R.

Objetivo de la norma

2. La NIA-ES 315R, como la NIA-ES 315 precedente, cubre los procedimientos del auditor para conocer la entidad y su entorno, el marco de información financiera aplicable y el sistema de control interno de la entidad, para poder identificar y valorar los riesgos de incorrección material.

El objetivo del auditor al llevar a cabo procedimientos para identificar y valorar los riesgos de incorrección material sigue siendo el mismo, es decir, identificar y valorar los riesgos de incorrección material, debida a fraude o error, tanto en los estados financieros como en las afirmaciones con la finalidad de proporcionar una base para el diseño y la implementación de respuestas a los riesgos valorados de incorrección material.[1]

¿Por qué se ha revisado la NIA-ES 315?

3. Conviene remontarnos al momento del nacimiento de la NIA 315. En 2003, tras varios años de trabajo, se aprobó la primitiva NIA 315, cuya redacción fue actualizada sin alterar su contenido esencial dentro del Clarity Project en 2006[2] que se ha mantenido vigente hasta la aprobación de la NIA 315(R2019) y hasta nuestros días en su versión española, hasta la aprobación de la NIA-ES 315R.

Esta NIA, que es la piedra angular de la actual metodología de auditoría de enfoque de riesgo, se ha mantenido prácticamente invariable durante casi 20 años mientras la realidad de las organizaciones

[1] Ver apartado 11 de la NIA-ES 315R.

[2] La IAASB abordó un estudio sobre su implantación y en 2013 concluyó que:

- Existía incoherencia en la naturaleza y el número de riesgos significativos identificados en la práctica.
- Obtener un conocimiento del sistema de control interno era difícil de realizar en la práctica.
- Los riesgos de las tecnologías de la información (TI) no se abordaron suficientemente en la norma.
- También se puso de relieve los desafíos de aplicar la NIA-ES 315 al auditar a las pequeñas y medianas entidades.

Fuente: IAASB (2022)

auditadas, en particular de las públicas, evolucionaba desde un entorno de gestión básicamente analógico de principios de siglo a los actuales entornos de administración electrónica avanzada, exclusivamente digitales, apoyados en redes interconectadas. Es decir, se había producido una disociación o brecha entre la NIA-ES 315 y la realidad del entorno donde deben aplicarla los auditores.

Pero, si profundizamos, la brecha es mucho mayor entre cómo se está aplicando la NIA-ES 315 en la práctica y las necesidades de auditar en un entorno digital en pleno siglo XXI.

La nueva NIA-ES 315 (Revisada) o NIA-ES 315R trata de cerrar esa brecha adaptando la norma a ese nuevo mundo plenamente digitalizado por una parte y por la otra abordando una serie de cuestiones que han dificultado la mencionada aplicación práctica de la NIA-ES 315 por los auditores.

En definitiva, como señala la IAASB (2019): "*La identificación y valoración del riesgo de incorrección material es fundamental para la auditoría. La NIA 315 (Revisada) Identificación y valoración del riesgo de incorrección material se ha revisado para exigir una identificación y valoración del riesgo más sólidas y, con ello, promover respuestas más adecuadas a los riesgos identificados. La norma ha sido revisada para responder a las dificultades y problemas detectados en la NIA 315 vigente introduciendo cambios dirigidos a una* ***mayor claridad y aplicación coherente****. Los requerimientos revisados se centran en "qué" se necesita hacer, y la guía de aplicación* ***mejorada, modernizada y reorganizada*** *en describir "por qué" y "cómo" se han de aplicar los procedimientos.*" Estas explicaciones pretenden aclarar ciertos requerimientos en los que puede haber habido malentendidos, aplicación incorrecta o aplicación incoherente en el pasado. Al incluir una explicación de por qué debían llevarse a cabo esos procedimientos, se pretende reducir el riesgo de aplicación incoherente de los requerimientos conexos.

En resumen, los cambios y los nuevos requisitos tienen por objeto aclarar y ayudar a identificar y valorar los riesgos de incorrección material (RIM) de una manera más consistente y sólida. Una vez identificados y valorados los RIM, la *NIA-ES-SP 1330 Respuestas del auditor a los riesgos valorados,* requiere que se diseñen y lleven a cabo procedimientos de auditoría posteriores para responder adecuadamente a esos RIM y que el auditor concluya si ha obtenido evidencia de auditoría suficiente y adecuada para emitir una opinión.

La calidad del proceso de identificación y valoración del riesgo tiene un efecto generalizado en todos los aspectos de la auditoría. Obtener un conocimiento de la entidad y su entorno, del marco de información financiera aplicable y del sistema de control interno de la entidad proporciona un marco de referencia dentro del cual el auditor identifica y valora los RIM.

Es importante resaltar que, aunque la nueva NIA-ES 315R ha sido revisada significativamente, **el modelo de riesgo de auditoría y su objetivo de identificar y valorar los riesgos de incorrección material en los estados financieros y en las afirmaciones, ya sea por fraude o error, no han cambiado.**

4. Mediante la revisión, reorganización y mejora de la norma actual, los cambios van dirigidos a:

   - Promover la coherencia en la aplicación de los procedimientos para la identificación y valoración del riesgo.
   - Hacer que la norma sea más graduable a través de unos requerimientos basados en principios.
   - Reducir la complejidad y hacerla más utilizable por los auditores de todo tipo de entidades, cualquiera que sea su naturaleza o complejidad.
   - Fomentar una valoración del riesgo más sólida y, con ello, unas respuestas más orientadas a esos riesgos identificados.
   - Ayudar a los auditores que utilizan la norma a manejar el efecto del uso de las TI por parte de los entes auditados en todos los aspectos de la metodología de auditoría, introduciendo guías de aplicación que reconocen el entorno cambiante en materia de tecnologías de la información incluyendo el uso de tecnologías emergentes. En especial a identificar y valorar los riesgos derivados del uso de TI.
   - Proporcionar orientaciones prácticas para la utilización de herramientas y técnicas automatizadas (HTA) en todas las etapas de la auditoría.
   - Alinear el contenido relativo al control interno con la estructura establecida por COSO 2013.

Conceptos clave de auditoría recogidos en NIA-ES 315R y nuevas definiciones

5. La NIA-ES-SP 1200*, Objetivos globales del auditor independiente y realización de la auditoría de conformidad con las normas internacionales de auditoría*, establece los objetivos generales del auditor en la ejecución de una auditoría de los estados financieros y explica la naturaleza y el alcance de la auditoría.

   Algunos de los conceptos clave de una auditoría se recogen en la NIA-ES 315R. En el cuadro siguiente se indica qué ha cambiado y qué no ha cambiado de algunos de esos conceptos clave:

Concepto clave	Sin cambios	Qué ha cambiado
Objetivo de la auditoría	**Obtener una seguridad razonable** de que los estados financieros en su conjunto están **libres de incorrecciones materiales,** debidas a fraude o error, que permita al auditor expresar una opinión y … emitir un **Informe.** El auditor debe de obtener **evidencia de auditoría adecuada y suficiente** para reducir el riesgo de auditoría a un nivel aceptablemente bajo.	Sigue siendo el mismo
Modelo de riesgo de auditoría	El riesgo de auditoría es el riesgo de que el auditor exprese una opinión de auditoría inadecuada cuando los estados financieros contengan incorrecciones materiales. Es una función del riesgo de incorrección material y del riesgo de detección. Los conceptos de riesgo inherente, riesgo de control y riesgo de detección descritos en la NIA-ES-SP 1200 no han cambiado.	El modelo general de riesgo de auditoría no ha cambiado. Ahora se requiere una **valoración separada** del riesgo inherente y del riesgo de control. Se han introducido los **factores de riesgo inherente** para ayudar a identificar y valorar los RIM. Se ha introducido el concepto de **espectro de riesgo inherente** para ayudar en la valoración del riesgo inherente.
Incorrección	Diferencia entre la cantidad, clasificación, presentación o información revelada respecto de una partida incluida en los estados financieros y la cantidad, clasificación, presentación o revelación de aplicable. Pueden deberse a errores o fraudes. Cuando el auditor manifiesta una opinión sobre si los estados financieros expresan la imagen fiel, o se presentan fielmente, en todos los aspectos materiales, las incorrecciones incluyen también aquellos ajustes que, a juicio del auditor, es necesario realizar en las cantidades, las clasificaciones, la presentación o la revelación de información para que los estados financieros expresen la imagen fiel o se presenten fielmente, en todos los aspectos materiales.	Definición de la NIA-ES-SP 1200.
Incorrección material	Se entiende por tal las producidas por errores o fraudes que suponen diferencias materiales entre lo contenido en la información financiera y, en su caso, presupuestaria, establecida por la regulación contable y presupuestaria, y lo recogido en los estados financieros o cuentas anuales auditadas. Estas diferencias pueden ser de cantidad, de clasificación, de presentación y de omisión o inclusión de información indebida.	Definición de la Nota explicativa de la NIA-ES-SP 1200.

6. Se han introducido varias definiciones nuevas, en el apartado 12 de la NIA-ES 315R, para ayudar a aclarar los requerimientos. Estas nuevas definiciones se señalan en la presente guía en tablas de color verde.

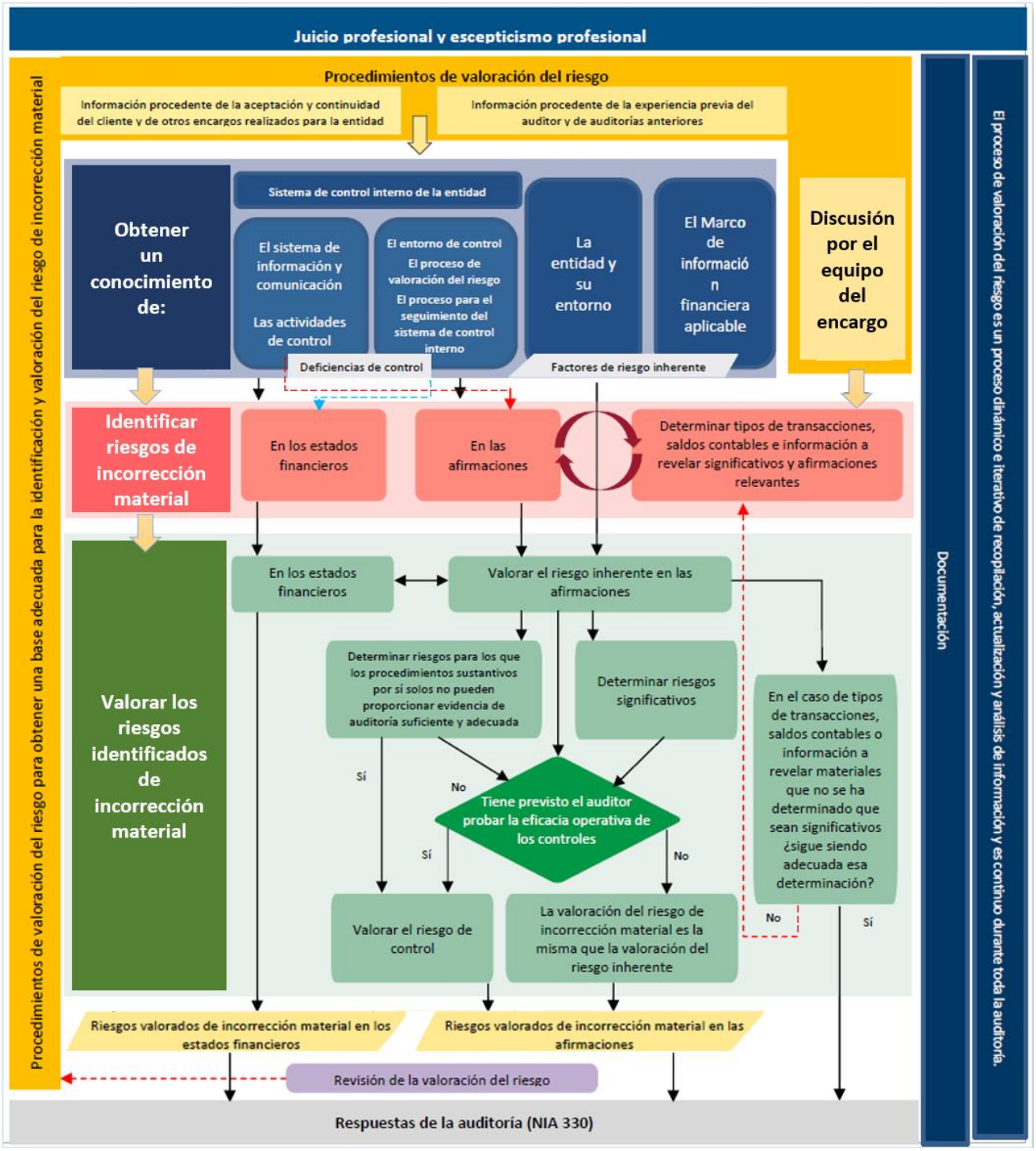
   También hay otros conceptos nuevos, como el *espectro de riesgo inherente,* diseñados para ayudar en la identificación y valoración del riesgo, que se explican a lo largo de la presente guía.

Naturaleza iterativa de la norma

7. **El proceso de identificación y valoración de los riesgos por el auditor es iterativo y dinámico**. *(Apartado 7 de la NIA-ES 315R)*

   El conocimiento por el auditor de la entidad y su entorno, del marco de información financiera aplicable y del sistema de control interno son interdependientes.

   En la obtención de conocimiento requerida por la NIA-ES 315R se pueden desarrollar expectativas iniciales de riesgos, las cuales pueden ser afinadas a medida que el auditor progresa en el proceso de identificación y valoración de riesgos. Normalmente se seguirán los siguientes pasos:



Fuente: IAASB, 2019

El diagrama de flujo anterior ilustra la naturaleza iterativa de la norma. Además, cuando la ejecución de ciertos requerimientos que se presentan antes dentro de la norma tienen dependencias de la ejecución de otros requerimientos presentados más adelante dentro de la norma, se ha agregado material de aplicación para hacer estas conexiones. Por ejemplo:

- El párrafo A49 de NIA-ES 315R explica que el auditor puede desarrollar expectativas iniciales sobre los tipos de transacciones, saldos contables e información a revelar (TTSCIR) que puedan ser significativos. Estos TTSCIR que se esperan significativos constituyen las bases del alcance del conocimiento del auditor del sistema de información de la entidad.
- El párrafo A127 señala además que el trabajo realizado en el sistema de información (conocimiento y evaluación) puede influir aún más en las expectativas del auditor sobre TTSCIR significativos.
- El párrafo A128 explica que **el conocimiento de los flujos de información en el sistema de información también puede ayudar a identificar los controles específicos que deben conocerse más a fondo en el componente actividades de control**.
- El párrafo A129 explica además que algunos controles solo pueden identificarse una vez que se hayan valorado los posibles riesgos de incorrección material.

Tanto la NIA-ES 315R como la NIA-ES-SP 1330 requieren que el auditor revise las valoraciones de riesgo, y modifique las respuestas globales posteriores y los procedimientos posteriores de auditoría, sobre la base de la evidencia de auditoría obtenida de la aplicación de procedimientos posteriores de auditoría de conformidad con la NIA-ES-SP 1330, o en caso de obtener nueva información.

Escepticismo profesional, obtención de evidencia libre de sesgos y juicio profesional

8. Se requiere que los auditores apliquen **escepticismo profesional** al diseñar y ejecutar los procedimientos de auditoría. Este importante concepto se ha reforzado, destacando que los procedimientos de valoración de riesgos deben diseñarse de una manera que **no esté sesgada** hacia la obtención de evidencia de auditoría corroborativa o la exclusión de la evidencia de auditoría contradictoria.

   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**. Además, cuando un tipo de transacciones, saldo contable o información a revelar es susceptible de incorrección debido a complejidad, subjetividad, cambio o incertidumbre, estos factores de riesgo inherente 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.

   Sobre la cuestión del riesgo de sesgo en la evidencia de auditoría, debe verse también la GPF-OCEX 1503.

   Independientemente de la fuente de información, el auditor considerará la relevancia y la fiabilidad de la información que vaya a utilizar como evidencia de auditoría de conformidad con el apartado 7 de la NIA-ES-SP 1500.

   El auditor está obligado a ejercer un **juicio profesional** en la planificación y ejecución de procedimientos de valoración de riesgos. Este concepto general no ha cambiado, pero se han realizado varias mejoras para ayudar al auditor a realizar juicios.

Graduación en la aplicación de la NIA-ES 315R

9. La NIA-ES 315R se aplica a la auditoría de los estados financieros de todo tipo de entidades, independientemente de su naturaleza, tamaño o complejidad.

   El concepto de graduación (es decir, poder aplicar las NIA-ES a entidades de diferentes tamaños y complejidades) es inherente a las NIAs, que siempre señalan lo que se puede hacer para ayudar a aplicarlas en todas las entidades. La norma revisada se centra en la complejidad y no en el tamaño, es decir, en «entidades menos complejas» en lugar de «entidades más pequeñas». Pero, aunque la dimensión de una entidad puede ser indicativa de su complejidad, algunas entidades de pequeña dimensión pueden ser complejas y algunas entidades de mayor dimensión pueden ser menos complejas.

La "***Guía de aplicación y otras anotaciones explicativas***" de la NIA-ES 315R incluye unos epígrafes denominados "*Graduación"* con numeroso material de aplicación en los que se exponen las cuestiones que se debe tener en cuenta al auditar **entidades de distinta complejidad**, y apoyan el ejercicio de juicios profesionales por el auditor en la determinación de los procedimientos de auditoría necesarios. La graduación se ha ilustrado en la norma mediante el uso de ejemplos de ambos extremos del espectro de complejidad.

Se debe tener presente el principio de proporcionalidad al auditar entidades de menor complejidad y tamaño, que en muchos OCEX son la mayoría de los casos.

Mayor claridad

10. Como se ha señalado, estudios de la IAASB habían llegado a la conclusión de que la estructura de la NIA 315 era muy compleja, con una deficiente organización de los temas y difícil de aplicar en la práctica.

Para paliar este problema **se ha reorganizado todo el material** para que sea más sencilla de aplicar. Se ha reordenado parte del material pasándolo a los anexos, que se han incrementado hasta seis. La guía de aplicación se ha mejorado, modernizado y reorganizado, y se han incluido numerosos ejemplos aclaratorios.

Para facilitar la comprensión se ha añadido al principio de la NIA-ES 315R un apartado nuevo denominado "Conceptos clave en esta NIA" que incluye referencias a otras NIA y recuerda una serie de conceptos básicos en la auditoría del enfoque de riesgo como: los objetivos globales de una auditoría financiera, cuáles son los componentes del riesgo de auditoría, para qué se valoran los riesgos, que el proceso de identificación y valoración del riesgo es continuo e iterativo, etc.

Los **anexos** de la NIA-ES 315R tienen la misma autoridad que la guía de aplicación (es decir, forman parte de la norma). La finalidad y el uso previsto de cada anexo se explican en su título o en los párrafos introductorios. Cada anexo tiene por objeto proporcionar orientación útil al auditor en el diseño y la realización de procedimientos de valoración de riesgos.

Los anexos se han utilizado para explicar en mayor medida cuestiones más directamente relacionadas con la entidad que se consideran útiles para el auditor en la realización de los procedimientos exigidos por la NIA-ES 315R. Por el contrario, los asuntos relacionados más directamente con las acciones del auditor sobre cómo aplicar los requerimientos están contenidos en la guía de aplicación.

Varias materias relacionadas con la entidad han sido **reubicadas** de la guía de aplicación de la NIA-ES 315 a los anexos de la nueva NIA-ES 315R, por ejemplo:

Anexo	Título
1	**Consideraciones para el conocimiento de la entidad y su modelo de negocio**
3	**Conocimiento del sistema de control interno de la entidad**
4	**Consideraciones para el conocimiento de la función de auditoría interna de la entidad**

Se han desarrollado **nuevos** anexos para ayudar en la aplicación de la norma:

Anexo	Título	Contenido
2	**Conocimiento de los factores de riesgo inherente**	Describe cómo afecta cada uno de los factores de riesgo inherentes (es decir, complejidad, subjetividad, cambio, incertidumbre y 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), y proporciona ejemplos de hechos o condiciones que pueden dar lugar a la existencia de RIM en las afirmaciones.

Anexo	Título	Contenido
5	**Consideraciones para el conocimiento de las Tecnologías de la Información (TI)**	Proporciona cuestiones adicionales que el auditor puede considerar para el conocimiento de la utilización de las TI en el sistema de control interno, incluyendo: • Asuntos a tener en cuenta al conocer el uso de TI por parte de la entidad en los componentes del sistema de control interno. • Ejemplos de características típicas de sistemas de información con diferentes complejidades. • Consideraciones en torno a la graduación. • Material de apoyo para la identificación de aplicaciones TI que están sujetas a riesgos derivados del uso de TI. • Otros aspectos del entorno de TI sujetos a riesgos derivados de la utilización de TI. • Identificación de riesgos derivados de la utilización de TI y CGTI
6	**Consideraciones para el conocimiento de los controles generales de TI**	Proporciona materias a considerar cuando se está conociendo los CGTI, incluyendo: • Descripción de la naturaleza de los CGTI. • Ejemplos de cómo los CGTI pueden abordar ejemplos de riesgos derivados del uso de TI.

¿Cuándo entra en vigor la NIA-ES 315R?

11. La NIA-ES 315R entra en vigor para períodos que comienzan a partir del 15 de diciembre de 2021. Es decir, en el sector privado será aplicable a partir de las auditorías del ejercicio 2022.

    Considerando que la NIA-ES 315R clarifica muchas cuestiones respecto de la NIA-ES 315, está mejor adaptada al entorno actual de trabajo de los OCEX y en buena parte de la metodología coincide con las GPF-OCEX, la Comisión Técnica de los OCEX ha propuesto que la **GPF-OCEX 1315 Revisada** sea aplicable en todas las auditorías que se inicien a partir del 1/1/2024 y **recomienda que se aplique** de forma voluntaria a las auditorías que se inicien a partir del 1/1/2023.

El enfoque de auditoría basado en el análisis de los riesgos

12. El auditor, al planificar una auditoría, debe identificar y valorar los riesgos de auditoría que pueden existir al ejecutar el trabajo y al emitir su informe. Teniendo en cuenta ese análisis debe diseñar un conjunto de procedimientos de forma que aborden esos riesgos y queden reducidos a un nivel aceptable a la hora de emitir el informe de auditoría. Es el denominado enfoque de auditoría basado en el análisis de los riesgos.

    De acuerdo con este enfoque, el objetivo del auditor es obtener una seguridad razonable de que las cuentas anuales en su conjunto están libres de incorrecciones materiales, debidas a fraude o error. Una seguridad razonable es un grado alto de seguridad y se alcanza cuando el auditor ha obtenido evidencia de auditoría suficiente y adecuada para reducir el riesgo de auditoría (es decir, el riesgo de expresar una opinión inadecuada cuando las cuentas anuales contengan incorrecciones materiales) a un nivel aceptablemente bajo. No obstante, una seguridad razonable no significa un grado absoluto de seguridad, debido a que existen limitaciones inherentes a la auditoría que hacen que la mayor parte de la evidencia de auditoría a partir de la cual el auditor alcanza sus conclusiones y en la que basa su opinión sea más convincente que concluyente[3].

    Así, este enfoque implica, básicamente, tres pasos:

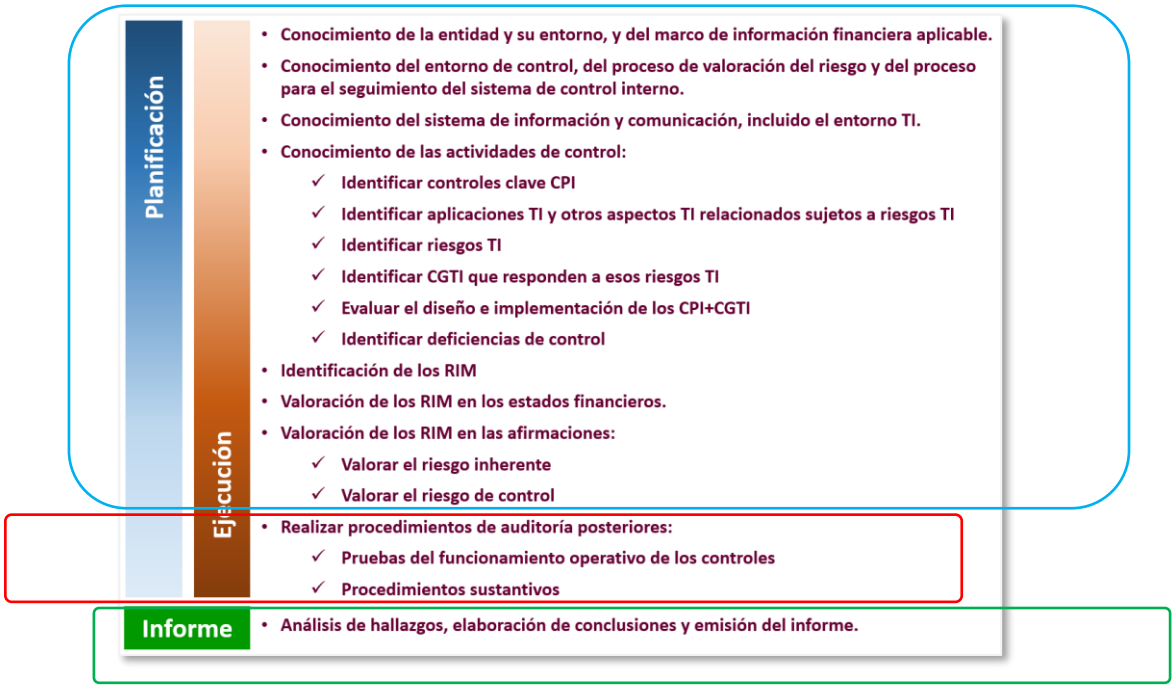
    a) Identificar y valorar el riesgo de incorrecciones materiales en las cuentas anuales (**GPF-OCEX 1315R**),

    b) Diseñar y ejecutar los procedimientos de auditoría precisos en respuesta a los riesgos valorados y reducir el riesgo de auditoría a un nivel aceptablemente bajo (**NIA-ES-SP 1330**), y

    c) Emitir un informe escrito basado en la evidencia de auditoría obtenida y en las conclusiones de auditoría a las que se ha llegado (**GPF-OCEX 1730**).

[3] Apartado 5 de la NIA-ES-SP 1200.

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



Debe tenerse presente que **la planificación de una fiscalización es un proceso continuo,** en el que, si bien la mayor parte de las actividades de planificación se realizan en las primeras etapas de la auditoría, debe reajustarse, siempre que sea necesario, a lo largo del trabajo.

Como se ha resaltado en el apartado 7 anterior, el proceso de identificación y valoración de los RIM es iterativo y dinámico, con interacciones entre los distintos pasos recogidos en el cuadro de arriba.

II Procedimientos de valoración del riesgo y actividades relacionadas
(apartados 13 a 18 de la NIA-ES 315R)

13. **La finalidad de realizar procedimientos de valoración del riesgo (PVR) es obtener evidencia de auditoría que proporcione una *base adecuada* para la identificación y valoración de los riesgos de incorrección material, y el diseño de procedimientos posteriores de auditoría en respuesta a esos riesgos.**[4]

Se enfatiza que la evidencia obtenida al realizar los PVR es, a todos los efectos, evidencia de auditoría. La intención con este cambio es ayudar a los auditores a comprender la naturaleza y extensión de lo que hay que hacer, es decir, ***se necesita suficiente evidencia adecuada*** para apoyar que las decisiones del auditor a partir de entonces respondan a los RIM valorados.

Es decir, para el diseño de procedimientos posteriores de auditoría se debe disponer de evidencia suficiente y adecuada que respalde esa decisión, es decir, **no se pueden diseñar y ejecutar los procedimientos posteriores de auditoría sin haber realizado previamente la valoración de riesgos**.

Los procedimientos de valoración del riesgo incluirán los siguientes[5]:

(a) **Indagaciones ante la dirección y ante otras personas apropiadas de la entidad,** incluidas personas de la función de auditoría interna (en caso de que exista esta función).

(b) **Procedimientos analíticos**

(c) **Observación e inspección.**

[4] Ver apartado 13 de la NIA-ES 315R.

[5] Ver apartado A14 de la NIA-ES 315R.

La naturaleza y la extensión de los PVR requeridos variarán en función de la naturaleza y las circunstancias de la entidad[6] (por ejemplo, el grado de formalización de sus políticas y procedimientos, así como de sus procesos y sistemas).

El auditor aplica su **juicio profesional** para determinar la naturaleza y extensión de los PVR que debe aplicar para cumplir los requerimientos de la NIA-ES.

En términos generales, aunque han sido reordenados, los requerimientos relacionados con la consideración de la **información de las actividades previas y de otros trabajos realizados** para el auditado, siguen siendo los mismos. El auditor tiene que considerar la información de la **experiencia previa con la entidad y las auditorías anteriores**[7]. En estos casos, el auditor no solo debe considerar la ***relevancia*** de la información, sino también su ***fiabilidad***.

Los temas a tratar en la **discusión de los riesgos por el equipo de la auditoría** siguen siendo en general los mismos, así como la necesidad de comunicarlos a los miembros del equipo que no participan en las discusiones.[8] Se puede utilizar el modelo de la GPF-OCEX 1513 para documentar esta importante reunión.

III 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)

14. En la NIA-ES 315R, **hay tres áreas principales que requieren el conocimiento del auditor:**

La obtención de conocimiento de la entidad y su entorno, del marco de información financiera aplicable y del sistema de control interno **es un proceso dinámico e iterativo de recopilación, actualización y análisis de información durante toda la auditoría**. En consecuencia, las expectativas del auditor pueden cambiar a medida que se obtiene nueva información.

Conocimiento de los factores de riesgo inherente

15. **El auditor debe aplicar PVR para obtener conocimiento del modo y el grado en que los factores de riesgo inherente 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**.[9]

Los factores de riesgo inherente son un **concepto nuevo** en la NIA-ES 315R (aunque ya se utilizó en la GPF-OCEX 1317) introducido para ayudar a los auditores a identificar los riesgos inherentes, para valorarlos y para que el auditor se centre en la susceptibilidad de las afirmaciones a incorrección.

Los factores de riesgo inherente se tendrán en cuenta **al valorar** el riesgo inherente. El auditor considerará el grado en que los factores de riesgo inherente 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.

[6] Ver apartado A16 de la NIA-ES 315R.
[7] Ver apartados 15 y 16 de la NIA-ES 315R
[8] Ver apartados 17 y 18 de la NIA-ES 315R
[9] Ver apartado 19.c) de la NIA-ES 315R.

Su definición:

	Nueva definición	Material explicativo adicional
Factores de riesgo inherente	**Características de hechos o condiciones que afectan la susceptibilidad de incorrección, debida a fraude o error, de una afirmación sobre un tipo de transacción, saldo contable u otra revelación, 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.	A7. Los factores de riesgo inherente pueden ser cualitativos o cuantitativos y afectar a la susceptibilidad de las afirmaciones a incorrección. 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. A8. 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 tipo de transacción, del saldo contable o de la información a revelar; • 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.

Un reflejo de la importancia que tiene este nuevo concepto es que aparece **43 veces** en la NIA-ES 315R.

El anexo 2 de la NIA-ES 315R describe los factores de riesgo inherente y proporciona ejemplos de hechos y condiciones que pueden indicar la existencia de RIM en las afirmaciones. También se ha añadido material adicional de aplicación (véanse los párrafos A85 a A89) para guiar al auditor a la hora de tener en cuenta esos factores, incluida la explicación de por qué se han introducido.

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.

Conocimiento de la entidad y su entorno

16. **El auditor aplicará procedimientos de valoración del riesgo para obtener conocimiento de los siguientes aspectos de la entidad y su entorno[10]:**

    (i) la estructura organizativa, de propiedad y de gobierno de la entidad y su modelo de negocio, incluido el grado en que el modelo de negocio integra el uso de TI

    (ii) factores sectoriales, normativos y otros factores externos y

    (iii) las mediciones utilizadas, interna y externamente, para valorar el resultado de la entidad.

    Para reconocer la evolución y la naturaleza cada vez más compleja del entorno en el que operan las entidades ahora, en el conocimiento de la entidad y su entorno, se enfatizan los aspectos relevantes del **modelo de negocio** de la entidad incluido el grado en que el modelo de negocio integra el **uso de TI** (véanse los párrafos A62 a A67).

    Este enfoque se amplía para incluir también el conocimiento por parte del auditor de cómo la entidad mide su **resultado financiero** (véanse los párrafos A74 a A81).

    Los cambios están destinados a que el auditor entienda realmente cómo opera la entidad, y sepa como mide sus resultados, desde el punto de vista de la administración, ya que eso puede ayudar al auditor a comprender dónde podrían surgir los RIM.

[10] Apartado 19.a de la NIA-ES 315R.

Se ha incluido un *Anexo 1 Consideraciones para el conocimiento de la entidad y su modelo de negocio*, en el que se explican los objetivos y el alcance del modelo de negocio de la entidad y se proporcionan ejemplos.

Conocimiento del marco de información financiera aplicable

17. **El auditor aplicará PVR para obtener conocimiento del marco de información financiera aplicable, así como las políticas contables de la entidad y los motivos de cualquier cambio en estas[11].**

    El auditor evaluará si las políticas contables de la entidad son adecuadas y congruentes con el marco de información financiera aplicable.[12]

    Los RIM se hacen evidentes a medida que la administración aplica los requerimientos de información financiera a las circunstancias de la entidad. Por lo tanto, esta es un área importante para el auditor, porque podrían derivarse RIM de cómo se aplica el marco de información financiera aplicable en esas circunstancias.

    La forma en que se aplica el marco de información financiera podría verse afectada por muchos factores, incluidos los factores de riesgo inherente, la competencia de quienes interpretan y aplican los requerimientos, así como la cantidad de interpretación necesaria para aplicarlos. Algunos o todos estos factores podrían dar lugar a RIM.

18. **El auditor aplicará PVR para obtener conocimiento del modo y el grado en que los factores de riesgo inherente 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[13].**

    Tener en cuenta los factores de riesgo inherente **al conocer** la entidad y su entorno, así como el marco de información financiera aplicable, tiene por objeto facilitar una identificación de riesgos más centrada y sólida, y ayudar a identificar dónde puede haber riesgos de posibles incorrecciones.

    También es necesario tener en cuenta los factores de riesgo inherente al considerar si existen aspectos del marco de información financiera que podrían dar lugar a un posible RIM. Por ejemplo, los requerimientos del marco de información financiera aplicable para las estimaciones contables pueden requerir que la administración utilice el juicio para formular estimaciones contables utilizando hipótesis sobre el futuro. En algunos casos, estas estimaciones pueden implicar una incertidumbre significativa y pueden ser complejas de calcular, en cuyo caso los factores de riesgo inherente de complejidad, subjetividad e incertidumbre en relación con las estimaciones contables de los estados financieros son relevantes. Esto, a su vez, podría dar lugar a la identificación de RIM dentro de la estimación contable.

Conocimiento del sistema de control interno de la entidad

19. La nueva NIA-ES-315R actualiza todos los aspectos relativos a los componentes de un sistema de control interno para adaptarlos a **COSO 2013**. Era un cambio necesario de un elemento importante para la auditoría, pero no es previsible que por sí mismo plantee ninguna dificultad especial de adaptación para los auditores.

    Aunque el enfoque para conocer el sistema de control de la entidad es en general el mismo que se requería en la NIA-ES 315 (es decir, conocer los 5 componentes del sistema de control interno), se han hecho muchos cambios sobre lo que este conocimiento implica para cada componente, y estos sí son importantes.

    Cada componente ha sido revisado para dejar claro «*qué*» debe conocerse, junto con los aspectos necesarios de la evaluación para obtener el conocimiento relevante. La guía de aplicación en la NIA-ES 315R explica *"por qué"* se requiere el conocimiento de los diversos componentes del sistema de control interno de la entidad (véanse los párrafos A97-A98 y A124-A125).

[11] Apartado 19.b de la NIA-ES 315R.

[12] Apartado 20 de la NIA-ES 315R.

[13] Apartado 19.c de la NIA-ES 315R.

Se actualizan las definiciones de varios conceptos importantes:

	Nuevas definiciones	Material explicativo adicional
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:** **(i) el entorno de control;** **(ii) el proceso de valoración del riesgo por la entidad;** **(iii) el proceso de la entidad para el seguimiento del sistema de control interno;** **(iv) el sistema de información y comunicación y** **(v) las actividades de control.**	Ver Anexo 3 de la NIA-ES 315 (Revisada).
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 contexto: (i) Las 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. (ii) Los procedimientos son actuaciones para implementar las políticas. *(Un **objetivo de control** hace frente a los riesgos existentes para alcanzar los objetivos de la entidad; proporciona una referencia específica contra la cual evaluar la eficacia de los controles en una auditoría.* *En los CPI se relaciona, generalmente, con una afirmación relevante y establece un criterio para evaluar si los procedimientos de control de la entidad proporcionan una seguridad razonable de que los controles evitan o detectan y corrigen oportunamente una incorrección u omisión en esa afirmación relevante referida a la información financiera y/o al cumplimiento de la legalidad.)*	Los controles están integrados en los componentes del sistema de control interno de la entidad. (A2) Las **políticas** 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. (A3) Los **procedimientos** 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. (A4) **Los controles pueden ser directos o indirectos**. Los controles directos son controles lo suficientemente precisos para responder a riesgos de incorrección material en las afirmaciones. Los controles indirectos son controles que sustentan los controles directos. (A5)
Controles de 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, validez y legalidad de las transacciones y otra información). *(Antes denominados **controles de aplicación**)*	Los CPI son procedimientos que sustentan la implementación eficaz de las políticas de información de la entidad. Los CPI pueden estar automatizados (es decir, incorporados en las aplicaciones de TI) o ser manuales (por ejemplo, controles de entrada o salida) y pueden depender de otros controles, incluidos otros controles de procesamiento de la información o en controles generales de TI. (A6) Ver apartado 33.

	Nuevas definiciones	Material explicativo adicional
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.	Ver Anexo 6 de la NIA-ES 315 (Revisada). Ver apartado 61.

20. Además de las definiciones anteriores, se han hecho varias aclaraciones al referirse a conceptos o términos específicos. La intención es que estas palabras se utilicen consistentemente para que no haya confusión en cuanto a lo que significa el concepto o término al aplicarlo:

(a) **El sistema de control interno de la entidad**

Se refiere a todo el sistema compuesto por los cinco componentes descritos en la definición.

(b) **Componente de actividades de control**

Este término solo se utiliza para describir el nombre del componente del sistema de control interno que incluye los controles individuales específicos que deben identificarse (es decir, el término «actividades de control» no se utiliza para nada más).

(c) **Controles**

Los controles son las *políticas y procedimientos* integrados dentro de los distintos componentes del sistema de control interno de la entidad. La NIA-ES 315R reconoce que estos pueden no estar formalizados o documentados, pero aún pueden ser evidentes a través de comunicaciones o implícitas a través de acciones y decisiones.

Los párrafos A156 a A157 establecen consideraciones para las **auditorías de entidades menos complejas** en las que los controles pueden operar de una manera menos formal. Sin embargo, a pesar de que las políticas y procedimientos en algunas entidades pueden estar menos formalizados, se requiere un conocimiento de esas políticas y procedimientos (en la medida necesaria para cumplir con los requerimientos de cada componente del sistema de control interno de la entidad) porque este conocimiento se necesita para la identificación y valoración de los RIM y las respuestas al mismo.

(d) **Controles indirectos**

Controles que no son lo suficientemente precisos para prevenir, detectar o corregir incorrecciones en las afirmaciones, pero **apoyan otros controles** y, por lo tanto, tienen un efecto indirecto en el funcionamiento adecuado de dichos controles.

(e) **Controles directos**

Controles suficientemente precisos para prevenir, detectar o corregir incorrecciones en las afirmaciones.

(f) **Control identificado (o control clave)**

Aquel que se ha identificado en las actividades de control por responder a un RIM en las afirmaciones.

(g) **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 y aprobadas formalmente, 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.[14]

[14] Un ejemplo sería la "Política de Seguridad de la Información", legalmente obligatoria para los entes públicos. Es un documento de alto nivel que define lo que significa "seguridad de la información" en una organización de acuerdo con el artículo 12 del Real Decreto 311/2022 y articula la gestión continuada de la seguridad TI.

(h) **Procedimiento o proceso**

Son actuaciones para implementar las políticas.

Conjunto organizado de actividades que se llevan a cabo para producir un producto o prestar un servicio, 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:

a) cómo llevar a cabo las tareas habituales,

b) quién debe hacer cada tarea y

c) cómo identificar y reportar comportamientos anómalos.

En muchas ocasiones los procesos o procedimientos estarán total o parcialmente automatizados.

Los procedimientos 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.

Para evitar confusiones, cuando el auditor describa o documente su conocimiento, se especificará claramente si el procedimiento está formalmente establecido y aprobado o no lo está. Los controles de seguridad de la información, básicamente CGTI, deben estar formalmente aprobados por exigencia del ENS.

(i) **Procesos de negocio o de gestión de una entidad**

Incluyen las actividades diseñadas para:

- el desarrollo, la adquisición, la producción, la venta y la distribución de los **productos 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 el sistema de información.

En el **Anexo 3 Conocimiento del sistema de control interno de la entidad** se describe con mayor detalle la naturaleza del sistema de control interno de la entidad y las **limitaciones inherentes** al control interno. También se proporciona una explicación adicional de los componentes de un sistema de control interno a efectos de las NIA.

21. El conocimiento requerido para cada componente del sistema de control interno está destinado a delinear los dos aspectos principales siguientes:

(a) Las cuestiones que el auditor debe conocer en relación con ese componente; y

(b) Una evaluación de esas cuestiones en el contexto de ese componente y de la naturaleza y circunstancias de la entidad.

Al realizar la evaluación de cada componente debe tenerse en cuenta que la forma en que se diseña, implementa y mantiene el sistema de control interno de la entidad varía con su tamaño y complejidad[15]. Por ejemplo, las entidades menos complejas pueden utilizar controles menos estructurados o más simples para lograr sus objetivos (y eso puede ser apropiado para esa entidad).

[15] Véase apartado A92 de la NIA-ES 315R.

22. Los 5 componentes del control interno se dividen en **dos tipos** que se alinean con la naturaleza de los controles dentro de cada componente, y pueden afectar a la identificación y valoración por parte del auditor de los RIM, así como a la respuesta a los riesgos valorados:

    (a) En el entorno de control, en el proceso de valoración de riesgos de la entidad y en el proceso de la entidad para el seguimiento de los componentes del sistema de control interno, los controles son principalmente **controles indirectos**[16]**,** aunque también puede haber algunos controles directos.

    (b) En los componentes del sistema de información y comunicación, y en las actividades de control, los controles son principalmente **controles directos**, es decir, controles lo suficientemente precisos para prevenir, detectar o corregir errores en las afirmaciones[17].

    Los controles indirectos influyen en la eficacia de los controles directos. Por ejemplo, el entorno de control es fundamental para todo el sistema de control interno, y si no funciona como se esperaba, esto afectaría a la eficacia de todos los controles de la entidad. Los CGTI son en general controles indirectos.

23. En la norma revisada se ha aclarado y mejorado el conocimiento de la **tecnología de la información (TI)** en relación con el sistema de control interno de la entidad y se destaca 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 (es decir, controles manuales y automatizados y otros recursos utilizados en el sistema de control interno de la entidad).[18]

Conocimiento del entorno de control (apartado 21 de NIA-ES 315R)

24. **El auditor obtendrá conocimiento del entorno de control que sea relevante para la preparación de los estados financieros mediante la aplicación de procedimientos de valoración del riesgo mediante:**

    (a) el conocimiento del conjunto de controles, procesos y estructuras que tratan:

    (i) el modo en que la dirección ejerce las responsabilidades de supervisión, tales como la cultura de la entidad y el compromiso de la dirección con la integridad y los valores éticos;

    (ii) la independencia de los responsables del gobierno de la entidad y su supervisión del sistema de control interno de la entidad cuando estos sean distintos de la dirección;

    (iii) la asignación de autoridad y responsabilidad en la entidad;

    (iv) el modo en que la entidad atrae, desarrolla y retiene personas competentes; y

    (v) el modo en que la entidad exige responsabilidades por la consecución de los objetivos del sistema de control interno a las personas que han de responder de ello; y

    (b) la evaluación de si:

    (i) la dirección, bajo la supervisión de los responsables del gobierno de la entidad, ha establecido y mantenido una cultura de honestidad y de comportamiento ético;

    (ii) el entorno de control proporciona una base adecuada para los demás componentes del sistema de control interno de la entidad considerando la naturaleza y complejidad de esta; y

    (iii) las deficiencias de control identificadas en el entorno de control menoscaban los demás componentes del sistema de control interno de la entidad.

    Las cuestiones específicas que deben conocerse para el entorno de control se incluyen ahora en un requerimiento, mientras que anteriormente algunos de estos asuntos solo se mencionaban dentro del material de aplicación. Es decir, **se exige que el auditor los conozca.**

    El párrafo A103 explica por qué se requiere la evaluación y enfatiza la naturaleza **fundamental** del componente del entorno de control para el resto de los componentes del sistema.

[16] Véase apartado A96 de la NIA-ES 315R.

[17] Véase apartado A123 de la NIA-ES 315R.

[18] Véase apartado A94 de la NIA-ES 315R.

25. La evaluación por el auditor del entorno de control en relación con la **utilización de TI** por la entidad puede incluir cuestiones tales como[19]:

    - Si la **gobernanza sobre las TI** es acorde con la naturaleza y complejidad de la entidad y de sus operaciones de negocio realizadas a través de TI, **incluida la complejidad o madurez de la plataforma o arquitectura tecnológicas de la entidad** y hasta qué punto confía la entidad en aplicaciones de TI para sustentar su información financiera.[20]
    - La **estructura organizativa** de la dirección en relación con las TI y los recursos asignados. Por ejemplo, **si la entidad ha invertido en un entorno de TI adecuado y en las mejoras necesarias, o si se ha contratado al suficiente número de personas con la cualificación adecuada** incluso cuando la entidad utiliza software comercial (con pocas o ninguna capacidad de modificación).

Conocimiento del proceso de valoración del riesgo por la entidad (apartados 22 y 23 de NIA-ES 315R)

26. **El auditor obtendrá conocimiento del proceso de valoración del riesgo por la entidad que sea relevante para la preparación de los estados financieros mediante la aplicación de PVR** a través de:

    (a) el conocimiento del proceso de la entidad para:

        i. la identificación de los riesgos de negocio relevantes para los objetivos de la información financiera;

        ii. la evaluación de la significatividad de dichos riesgos, incluida la probabilidad de ocurrencia y

        iii. la respuesta a dichos riesgos; y

    (b) la evaluación de si el proceso de valoración del riesgo por la entidad es adecuado a las circunstancias de la entidad teniendo en cuenta la naturaleza y complejidad de esta.

    Los asuntos específicos que deben conocerse del proceso de valoración del riesgo por la entidad son similares a los requeridos en la NIA-ES 315. El párrafo A111 explica por qué el auditor debe evaluar si el proceso de valoración de riesgos de la entidad es apropiado.

Conocimiento del proceso de la entidad para el seguimiento del sistema de control interno (apartado 24)

27. **El auditor obtendrá conocimiento del proceso de la entidad para el seguimiento del sistema de control interno relevante para la preparación de los estados financieros, mediante la aplicación de PVR** a través de:

    (a) el conocimiento de los aspectos del proceso de la entidad que tratan de:

        (i) las evaluaciones continuas e individuales para el seguimiento de la eficacia de los controles y la identificación y corrección de las deficiencias de control identificadas; y

        (ii) en su caso, la función de auditoría interna, incluida su naturaleza, responsabilidades y actividades;

    (b) el conocimiento de las fuentes de información utilizadas en el proceso de la entidad para el seguimiento del sistema de control interno, y los fundamentos de la dirección para considerar que la información es suficientemente fiable para esa finalidad; y

    (c) la evaluación de si el proceso de seguimiento del sistema de control interno de la entidad es adecuado a las circunstancias de la entidad teniendo en cuenta la naturaleza y complejidad de esta.

    El enfoque se centra en el *proceso* de la entidad para el seguimiento del sistema de control interno, esto incluye conocer previamente las principales actividades que la entidad utiliza para su seguimiento.

    Al igual que con los demás componentes del control interno en la NIA-ES 315R se requiere una evaluación del proceso que la entidad tiene en marcha teniendo en cuenta la naturaleza y las circunstancias de la entidad. El párrafo A120 explica que tener en cuenta las fuentes de información que la entidad utiliza para el seguimiento de los controles ayuda a comprender si el proceso en sí es apropiado para esa entidad.

[19] Véase apartado A108 de la NIA-ES 315R.

[20] Véase GPF-OCEX 5331 Gobernanza corporativa, gobernanza sobre las TI y su auditoría.

Conocimiento del sistema de información y comunicación (SIC) (apartado 25 de NIA-ES 315R)

28. **El auditor obtendrá conocimiento del SIC de la entidad que sea relevante para la preparación de los estados financieros, mediante la aplicación de procedimientos de valoración del riesgo a través de:**

    (a) **el conocimiento de las actividades de procesamiento de la información de la entidad, incluidos sus datos e información, los recursos que se deben utilizar en esas actividades y las políticas que definen, para los TTSCIRS:**

        i. el modo en que la información fluye[21] por el SI de la entidad, incluido el modo en que:

            a. las transacciones se inician y la información sobre ellas se registra, se procesa, se corrige si es necesario, se traslada al mayor y se incluye en los estados financieros; y

            b. la información sobre los hechos y condiciones, distintos de las transacciones, se captura, se procesa y se revela en los estados financieros;

        ii. los registros contables, cuentas específicas de los estados financieros y otros registros de soporte relacionados con los flujos de información en el sistema de información;

        iii. el proceso de información financiera utilizado para la preparación de los estados financieros de la entidad, incluida la información a revelar; y

        iv. **los recursos de la entidad, incluido el entorno de TI**, relevantes para los apartados i a iii anteriores;

    (b) el conocimiento del modo en que la entidad comunica las cuestiones significativas que sustentan la preparación de los estados financieros y las correspondientes responsabilidades de información en el sistema de información y otros componentes del sistema de control interno:

        i. a personas dentro de la entidad, incluido el modo en que se comunican las funciones y responsabilidades relacionadas con la información financiera;

        ii. a la dirección y los responsables del gobierno de la entidad y

        iii. con terceros, tales como las realizadas con las autoridades reguladoras; y

    (c) **la evaluación de si el SIC de la entidad sustenta adecuadamente** la preparación de los estados financieros de conformidad con el marco de información financiera aplicable.

29. Para ayudar a determinar el alcance del conocimiento necesario, la NIA-ES 315R requiere **que se conozcan las actividades de procesamiento de información para cada TTSCIRS.**

    Aunque la determinación de los TTSCIRS se aborda más adelante en la norma, el auditor puede tener una expectativa preliminar de los TTSCIR que son significativos. Desde un punto de vista práctico esa expectativa preliminar puede establecerse al analizar inicialmente las cuentas anuales a auditar y al calcular los niveles de importancia relativa. Si posteriormente resultan TTSCIRS adicionales, el auditor tendría que obtener el conocimiento pertinente de esa parte del sistema de información.

    Además de conocer los datos y la información, también se debe conocer todos los **recursos** que la entidad va a utilizar en las actividades de procesamiento de la información[22] incluyendo aspectos sobre recursos humanos que pueden ser relevantes (como la **competencia profesional de las personas que realizan el trabajo, si se dispone de los recursos adecuados y si existe una adecuada segregación de funciones**). También incluye los recursos informáticos y cuestiones conexas, que se explican más adelante.

    La obtención de **conocimiento de los procesos de negocio/gestión de la entidad**, que incluye el modo en que se originan las transacciones, ayuda al auditor en la obtención de conocimiento del sistema de información de la entidad de un modo adecuado a las circunstancias de la entidad. (A135 de NIA-ES 315R).

[21] Para documentar el modo en la que la información fluye por el sistema de información se utilizarán flujogramas realizados acorde con la *GPF-OCEX 1512 Cómo realizar mapas de procesos y flujogramas*.

[22] Apartado A133 de la NIA-ES 315R.

Para obtener este conocimiento el auditor podrá realizar(A136):

- indagaciones ante el personal relevante acerca de los procedimientos utilizados para iniciar, registrar, procesar las transacciones e informar sobre ellas o sobre el proceso de información financiera;
- la inspección de manuales de políticas o procesos u otra documentación del SI de la entidad;
- la observación de la ejecución de las políticas o procedimientos por el personal de la entidad; o
- comprobaciones paso a paso (ver para ello la GPF-OCEX 1311).

30. **La utilización de tecnologías de la información en el sistema de información (SI)**.

Como parte de la valoración del riesgo, la NIA-ES 315R requiere de forma explícita que el auditor obtenga un conocimiento de los sistemas de información relevantes para la preparación de las cuentas anuales y del sistema de control interno de la entidad con la finalidad de identificar y valorar los RIM. Esto incluye comprender el uso de la tecnología de la información por parte de la entidad e identificar los riesgos derivados del uso de la tecnología de la información.

En términos generales, el auditor debe conocer los siguientes aspectos de TI del **sistema de información**[23]:

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

(b) **Se debe conocer el entorno TI** relevante para los flujos de transacciones y el procesamiento de la información en el sistema de información de la entidad **porque la utilización de aplicaciones de TI u otros aspectos del entorno de TI pueden dar lugar a riesgos derivados de la utilización de TI.**

(c) Se debe identificar y comprender **la naturaleza y el número de las aplicaciones específicas de TI, 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

Los cambios en los flujos de transacciones o en la información dentro del sistema de información pueden ser el resultado de cambios en los programas de las aplicaciones de TI o de cambios directos en los datos de las bases de datos que intervienen en el procesamiento o en el almacenamiento de esas transacciones o información.

Para más detalle sobre los aspectos TI ver el apartado **V** siguiente.

31. El conocimiento por el auditor del SI incluye el entorno de TI relevante para los flujos de transacciones y el procesamiento de la información en el SI de la entidad porque la utilización de aplicaciones de TI u otros aspectos del entorno de TI pueden dar lugar a **riesgos derivados de la utilización de TI**.

El **entorno de las TI** está formado por[24]:

a) **Aplicaciones TI,** son programas que se utiliza para el inicio, procesamiento, registro y reporte de transacciones o información. Las aplicaciones de TI incluyen almacenes de datos y generadores de informes.

b) La **infraestructura de TI** que da soporte a las TI comprende el hardware y software relacionados con:
   - ✓ la red,
   - ✓ los sistemas operativos y
   - ✓ las bases de datos.

c) Los **procesos de TI** son los procesos de la entidad para la gestión del acceso al entorno de TI, la gestión de cambios en los programas o de los cambios al entorno de TI, y para la gestión de las operaciones TI.

d) El **personal de TI** involucrado en esos procesos que una entidad utiliza para respaldar las operaciones de negocio y para lograr la consecución de las estrategias de negocio.

[23] Apartados A140-A143 de la NIA-ES 315R.

[24] Apartado 12.(g) de la NIA-ES 315R.

***Conocimiento de las actividades de control (apartado 26 de la NIA-ES 315R)*[25]**

32. Hasta ahora se exigía que el auditor identificara las **actividades de control relevantes** para la auditoría[26], **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.

La nueva NIA-ES 315R **elimina el concepto de controles relevantes** para la auditoría y en el apartado 26 es mucho más específica y **concreta los controles que el auditor debe conocer obligatoriamente**.

	Ver apartado
El auditor debe obtener conocimiento del componente de actividades de control, en particular debe:	
a) Identificar los controles que responden a los RIM en las afirmaciones:	
i Los **controles que responden a un riesgo que se considera riesgo significativo**.	33
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.	
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**.	34
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.	35
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 (a).	36 37
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.	38 39

La NIA-ES 315R establece una secuencia lógica en el conocimiento de las actividades de control:

33. **Identificar los controles que responden a los RIM en las afirmaciones**

La identificación y evaluación por el auditor de controles en el componente de actividades de control se centrará en los **controles de procesamiento de la información (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[27].** A estos objetivos, en el sector público hay que añadir el de **legalidad**.

Para conocer y revisar estos CPI, se desarrolló y aprobó la ***GPF-OCEX 5340 Los controles de aplicación: qué son y cómo revisarlos,*** en la cual se señala que "*el objetivo de la auditoria de los controles de aplicación será obtener una seguridad razonable de que el sistema de control interno garantiza la completitud, exactitud, validez y legalidad de las transacciones y datos registrados en la aplicación de gestión revisada y su posterior contabilización; es decir, si la eficacia de los controles relevantes garantiza la correcta ejecución de los procesos de gestión auditados y mitigan el riesgo de errores e irregularidades*."

[25] Para una mejor comprensión, se recomienda leer con carácter previo el apartado **IV Identificación y valoración del RIM**.
[26] Apartado 20 de la anterior NIA-ES 315.
[27] Apartado A148 de la NIA-ES 315R.

En el siguiente cuadro se amplía esta información sobre los objetivos de los CPI:

Objetivos de los CPI	Descripción (según la GPF-OCEX 5340)
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, reconciliaciones, 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.*
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.

No se requiere que el auditor identifique y evalúe todos los CPI relacionados con las políticas de la entidad que definen los flujos de transacciones y otros aspectos de las actividades de procesamiento de la información para los TTSCIRS[28], **se centrará en los que responden a los RIM**.

34. Los planes del auditor de probar la **eficacia operativa de los controles** (apartado 26.a.iii) también pueden verse influidos por los riesgos identificados de incorrección material en los estados financieros. *Por ejemplo*, si se identifican deficiencias en el entorno de control, esto puede afectar a las expectativas globales acerca de la eficacia operativa de los controles directos.[29]

    Ver también el punto 53 siguiente.

35. El auditor, basándose en su juicio profesional, puede considerar adecuado identificar **otros controles**[30], evaluar su diseño y determinar su implementación. Entre estos estarán:

    - 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 auxiliares con el mayor o,
    - en el caso de utilizar una organización de servicios, controles complementarios de la entidad usuaria[31]. Si se utilizan servicios de computación en la nube se tendrá en consideración la GPF-OCEX 1403.

[28] Apartado A148 de la NIA-ES 315R.
[29] Apartado A164 de la NIA-ES 315R.
[30] Apartados 26.a.iv y A165 de la NIA-ES 315R.
[31] Véase la NIA-ES 402, *Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios.*

36. **Identificación de las aplicaciones TI sujetas a riesgos derivados de la utilización de TI**

Se tratará de aquellas aplicaciones relacionadas procesos de negocio que soportan los TTSCIRS, en las que se han identificado CPI y que están sujetas a riesgos derivados de la utilización de TI.

La identificación de las aplicaciones sujetas a riesgos derivados de la utilización de TI implica tener en cuenta los CPI identificados por el auditor puesto que tales controles pueden suponer la utilización de TI o confiar en las TI. El auditor se puede centrar en si una aplicación de TI incluye controles automatizados en los que confía la dirección identificados por él, incluidos los controles que responden a riesgos para los cuales los procedimientos sustantivos por sí solos no proporcionan evidencia de auditoría suficiente y adecuada. El auditor también puede considerar el modo en que la información relativa a los tipos de transacciones, saldos contables e información a revelar se almacena y procesa en el sistema de información y si la dirección confía en controles generales de TI para mantener la integridad de esta.

La amplitud del conocimiento del auditor de los procesos de TI, incluido el grado en que la entidad ha establecido CGTI, variará según la naturaleza y las circunstancias de la entidad y de su entorno de TI, así como según la naturaleza y extensión de los controles identificados por el auditor. El número de aplicaciones de TI sujetas a riesgos derivados de la utilización de TI también variará en base a estos factores.

***Ejemplos** (A170):*

- *Es poco probable que una entidad que utiliza un software comercial y no tiene acceso al código fuente para realizar ningún cambio en los programas tenga un proceso relativo a cambios en los programas, pero sí puede tener procedimientos para configurar el software (por ejemplo, el cuadro de cuentas, parámetros, etc). Además, es posible que la entidad tenga un proceso o procedimientos para gestionar el acceso a la aplicación (por ejemplo, haber nombrado una persona para que tenga acceso al software comercial). En esas circunstancias, es poco probable que la entidad tenga o necesite CGTI formales.*
- *Por el contrario, es posible que una entidad de gran dimensión confíe en mayor grado en las TI y el entorno de TI puede involucrar múltiples aplicaciones de TI y los procesos de TI para la gestión del entorno de TI pueden ser complejos), incluido el que la entidad haya implementado CGTI formales sobre sus procesos de TI.*
- *Cuando la dirección no confíe en controles automatizados o en CGTI para el procesamiento de transacciones o el mantenimiento de los datos, y el auditor no haya identificado ningún control automatizado u otros controles de procesamiento de la información (o ninguno que dependa de los CGTI), el auditor puede planificar comprobar directamente cualquier información generada por la entidad que implique TI y puede no identificar ninguna aplicación de TI sujeta a riesgos por la utilización de TI. Esto solo será probable en entes pequeños y poco complejos.*
- *Cuando la dirección confíe en una aplicación de TI para el procesamiento o el mantenimiento de los datos y el volumen de datos sea significativo, la aplicación de TI ejecute controles automatizados que el auditor también ha identificado, es probable que la aplicación de TI esté sujeta a riesgos por la utilización de TI.*

37. **Identificación de otros aspectos del entorno de TI sujetos a riesgos derivados de la utilización de TI.**[32]

Los otros aspectos del entorno de TI que pueden estar sujetos a riesgos derivados de la utilización de TI incluyen la red, los sistemas operativos y bases de datos y, en determinadas circunstancias, las comunicaciones (interfaces) entre aplicaciones de TI y con la nube.

Por lo general, **no se identifican otros aspectos del entorno de TI cuando el auditor no identifica aplicaciones sujetas a riesgos derivados de la utilización de TI**.

Cuando el auditor haya identificado aplicaciones de TI sujetas a riesgos derivados de la utilización de TI, es probable que se identifiquen otros aspectos del entorno de TI (por ejemplo, bases de datos, sistema operativo, red) porque esos aspectos dan apoyo e interactúan con las aplicaciones de TI identificadas.

38. **Identificación de riesgos derivados de la utilización de TI** (Apartado 26.c y A173)

En la identificación de riesgos derivados de la utilización de TI, el auditor puede considerar la naturaleza de la aplicación de TI identificada u otro aspecto del entorno de TI y los motivos por los que están sujetos a riesgos derivados de la utilización de TI.

En el caso de algunas aplicaciones de TI u otros aspectos del entorno de TI identificados, es posible que el auditor identifique riesgos aplicables derivados de la utilización de TI relacionados principalmente con accesos no autorizados o con cambios no autorizados en los programas, o que tratan los riesgos de cambios

[32] Apartado 26.b y A167-A172

inapropiados en los datos (por ejemplo, el riesgos de cambios inapropiados en los datos mediante el acceso directo a las bases de datos o la capacidad de manipular directamente la información).

La extensión y la naturaleza de los riesgos aplicables identificados derivados de la utilización de TI varían según la naturaleza y las características de las aplicaciones de TI y otros aspectos del entorno de TI.

Se pueden producir riesgos de TI cuando la entidad emplea **proveedores de servicios** externos o internos para algunos aspectos de su entorno de TI (por ejemplo, subcontratando a un tercero para el alojamiento de su entorno de TI o utilizando un centro de servicios compartidos para la gestión centralizada de los procesos de TI en un grupo). Riesgos derivados de la utilización de TI también se pueden identificar en relación con la **ciberseguridad**.

Es más probable que haya más riesgos derivados de la utilización de TI cuanto mayor sea el volumen o la complejidad de los controles de aplicaciones automatizados y la dirección otorgue una mayor confianza a dichos controles para un procedimiento eficaz de las transacciones o el mantenimiento eficaz de la integridad de la información subyacente.

39. **Identificación de los CGTI de la entidad que responden directamente a los riesgos TI** (Apartado 26.c)

En el apartado 26.c) de la NIA-ES 315R se requiere que el auditor **identifique los CGTI** relacionados con los riesgos TI porque **los CGTI sustentan el funcionamiento continuo y eficaz de los CPI**. Un CGTI, solo, no es habitualmente suficiente para responder a un riesgo de incorrección material en las afirmaciones.[33]

Más adelante, en el apartado V, se analiza la cuestión de los CGTI.

40. **Evaluar el diseño e implementación (D+I) de los controles** (Apartado 26.d)

Adicionalmente para cada uno de los controles (CPI+CGTI) identificados el auditor debe[34]:

a) Evaluar si el control está diseñado eficazmente para responder al RIM en las afirmaciones o si está diseñado eficazmente para sustentar el funcionamiento de otros controles.

b) Determinar si el control ha sido implementado.

La **evaluación del diseño de un control (D)** implica la consideración por el auditor de 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).[35]

El auditor determina la **implementación de un control (I)** estableciendo que el control existe y que la entidad lo está utilizando. 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**. Un control incorrectamente diseñado puede representar una **deficiencia de control**[36].

Evaluar el diseño y determinar la implementación (D+I) de controles identificados en el componente de actividades de control no es suficiente para comprobar su eficacia operativa. Sin embargo, **en el caso de controles automatizados, el auditor puede planificar comprobar su eficacia operativa de los controles automatizados mediante la identificación y comprobación de CGTI que aseguran el funcionamiento congruente de un control 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 controles automatizados**[37].

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 la NIA-ES-SP 1330 (apartados 8 a 11) se describen con más detalle las pruebas sobre la eficacia operativa de los controles, incluidas las pruebas de controles indirectos.

[33] Apartado A150 de la NIA-ES 315R.
[34] Apartado 26.d) de la NIA-ES 315R.
[35] Apartado A175 de la NIA-ES 315R.
[36] Apartado A176 de la NIA-ES 315R.
[37] Apartado A180 de la NIA-ES 315R.

41. **Por qué el auditor identifica los riesgos derivados de la utilización de TI y los controles generales relacionados con aplicaciones de TI identificadas y otros aspectos del entorno de TI** (A166).

El conocimiento de los **riesgos derivados de la utilización de TI y de los controles implementados por la entidad para responder a esos riesgos** puede afectar a:

- la decisión del auditor sobre si probar la eficacia operativa de los controles 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 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 correspondiente 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.*

- la valoración por el auditor del riesgo inherente en las afirmaciones; o

  Ejemplo*: Cuando hay cambios significativos y extensos en los programas de una aplicación de TI para tratar requerimientos de información nuevos o revisados del marco de información financiera aplicable, puede ser un indicio de la complejidad de los nuevos requerimientos 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.*

- el diseño de procedimientos posteriores de auditoría.

  Ejemplo: *Si los CPI dependen de los CGTI, es posible que el auditor decida comprobar la eficacia operativa de los CGTI, para lo que será necesario diseñar pruebas de controles para esos controles generales. Si, en las mismas circunstancias, el auditor determina no comprobar la eficacia operativa de los CGTI o se espera que dichos controles generales sean ineficaces, los riesgos relacionados derivados de la utilización de TI probablemente tengan que ser tratados mediante el diseño de procedimientos sustantivos. No obstante, es posible que los riesgos derivados de la utilización de TI no puedan ser tratados cuando están relacionadas con riesgos para los cuales los procedimientos sustantivos por sí solos no proporcionan evidencia de auditoría suficiente y adecuada. En esas circunstancias, es posible que el auditor deba considerar las* ***implicaciones en la opinión del auditor****.*

Deficiencias de control (párrafo 27 de la NIA-ES 315R)

42. **Basándose en su evaluación de cada uno de los componentes del sistema de control interno de la entidad, el auditor determinará si se han identificado una o más deficiencias de control[38].**

Al realizar las evaluaciones de cada uno de los componentes del sistema de control interno de la entidad[39], es posible que el auditor determine que algunas de las políticas de la entidad o los procedimientos en un componente no son adecuadas a la naturaleza y las circunstancias de la entidad. Esta determinación puede ser un indicador que ayude al auditor a identificar **deficiencias de control**. Si el auditor ha identificado una o varias deficiencias de control, puede tener en cuenta el efecto de esas deficiencias para el diseño de procedimientos posteriores de auditoría de conformidad con la NIA-ES-SP 1330.[40]

Si el auditor llega a la conclusión de que los controles no están diseñados adecuadamente para prevenir, detectar y corregir una incorrección importante, o no se han aplicado correctamente durante el periodo

[38] Apartado 27 de la NIA-ES 315R.

[39] Apartados 21(b), 22(b), 24(c), 25(c) y 26(d)

[40] Apartado A182 de la NIA-ES 315R.

auditado, deberá determinar si, individualmente o en combinación, las deficiencias constituyen una **deficiencia significativa**[41] con arreglo a la NIA-ES-SP 1265/GPF-OCEX 1265, comunicar las deficiencias en el control interno a los encargados de la gobernanza y la dirección, y puede ser necesario tener en cuenta el efecto de la deficiencia de control en el diseño de procedimientos posteriores de auditoría de conformidad con la NIA-ES-SP 1330 (es decir, qué impacto puede tener la deficiencia en el enfoque de auditoría).

IV Identificación y valoración del RIM *(apartados 28 a 37 de la NIA-ES 315R)*

43. La NIA-ES 315R ha separado los requerimientos para identificar los RIM de los requerimientos para valorarlos con la finalidad de desarrollar un marco para que los auditores identifiquen y valoren los RIM de manera sólida.

Las nuevas definiciones relacionadas son:

	Nuevas definiciones	Material explicativo adicional
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. Las afirmaciones son distintas de las manifestaciones escritas requeridas por la NIA 580 para confirmar determinadas cuestiones o sustentar otra evidencia de auditoría. (A1)
Afirmación relevante	**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, el riesgo inherente).	Un riesgo de incorrección material puede estar relacionado con más de una afirmación, en cuyo caso, todas las afirmaciones con las que se relaciona dicho riesgo son afirmaciones relevantes. Si una afirmación no tiene un riesgo identificado de incorrección material, no se trata de una afirmación relevante. (A9)
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.**	*La NIA-ES 315R ha traducido "relevant assertion" indistintamente como "**afirmación significativa**" y como "**afirmación relevante**", por tanto, tienen el **mismo significado**.*
Riesgo de incorrección material	**Riesgo de que los estados financieros contengan incorrecciones materiales antes de la realización de la auditoría.** **El riesgo comprende dos componentes,** descritos del siguiente modo, en las afirmaciones**:** i **Riesgo inherente:** 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.	Definición dada en la NIA-ES-SP 1200, apartado 13.n). Aunque la definición del riesgo de incorrección material no ha cambiado, en la *guía de aplicación* de la ISA 200, nuevo *párrafo A15.a* (pendiente de trasladar a España) se ha aclarado que *"existe un riesgo de incorrección material cuando hay una **posibilidad razonable** de que: (a) exista una incorrección (es decir, su probabilidad de existir) (b) en caso de que exista, sea material (es decir, su magnitud)"*.

[41] Apartado A183 de la NIA-ES 315R.

	Nuevas definiciones	Material explicativo adicional
	ii Riesgo de control: 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.	Basándose en esta aclaración, el término ***probabilidad razonable*** se utiliza en el párrafo A186 de la NIA-ES 315R en lo que respecta al umbral para identificar los riesgos de incorrección material.
Riesgo significativo	**Es un riesgo identificado de incorrección material** **i) 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 ii) que deba ser tratado como riesgo significativo de conformidad con los requerimientos de otras NIA.	La significatividad se puede describir como la importancia relativa de una cuestión y el auditor la juzga en el contexto en la que se está considerando. Para el riesgo inherente, la significatividad se puede considerar en el contexto de cómo y en qué grado los **factores de riesgo inherente** afectan a la combinación de la **probabilidad** de que exista una incorrección material y a la **magnitud** de la incorrección potencial si existe. (A10)

Los **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.

Una vez que el auditor conoce los tipos de transacciones significativas y las operaciones que las generan, se concentrará en ellas y puede proceder al análisis de riesgos en las diferentes fases del proceso de gestión en el que se producen tales operaciones.

Las **transacciones no rutinarias**, como las estimaciones, operaciones de consolidación, ajustes de final de ejercicio, etc. son revisadas normalmente mediante procedimientos sustantivos.

Las afirmaciones y su utilización[42]

44. **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**.

Las afirmaciones para las que el auditor ha identificado riesgos relacionados de incorrección material son afirmaciones relevantes.

En la anterior NIA-ES 315 las afirmaciones eran un elemento esencial para identificar y valorar los RIM y diseñar respuestas a esos riesgos, pero su utilización no estaba bien explicada y no resultaba sencillo para los auditores utilizarlas en la práctica de una forma adecuada.

Las afirmaciones siguen siendo básicamente las mismas y no hay ninguna novedad sustancial sobre lo que ya conocemos de la NIA-ES 315 y GPF-OCEX 1317, pero la definición se ha matizado un poco para hacerla más comprensible.

La novedad principal consiste en que **la importancia de las afirmaciones queda muy reforzada** en la NIA-ES 315R al detallar exhaustivamente su utilización a lo largo del proceso auditor. Baste decir como reflejo de esa importancia reforzada que la nueva norma menciona ese término **142 veces contra 41** en la versión anterior.

Igual que sucedía hasta ahora, la NIA 315R señala que en las auditorías del sector público se tendrá en consideración la afirmación de legalidad, es decir la afirmación implícita de que las transacciones y hechos se han desarrollado de conformidad con las disposiciones legales. Aunque este apartado ha sido eliminado en la NIA-ES 315R por ser esta de aplicación para el sector privado, los auditores públicos debemos recuperarlo para su aplicación en nuestro trabajo tal como establece la ISSAI 1315 y la GPF-OCEX 1317. En

[42] Apartados A188-A191 de la NIA-ES 315R.

la GPF-OCEX 1315R se han recuperado todos estos apartados eliminados relativos al sector público.

Ya se ha mencionado antes una cuestión relativa a la traducción. Se mantiene el mismo error de traducción que en la versión anterior y sobre el que se debe tener cuidado para evitar confusiones. Se ha traducido la afirmación "completeness" por integridad, lo cual en el contexto de la NIA puede ocasionar confusión. Por eso en la GPF-OCEX 1315R se ha utilizado integridad y completitud, de acuerdo con el original en inglés, para distinguir claramente estos dos diferentes conceptos.

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

	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.

Identificación de los riesgos de incorrección material *(párrafos 28 y 29 de la NIA-ES 315R)*

45. Como se ha señalado anteriormente, **el modelo de riesgo de auditoría no ha cambiado.**

El auditor está obligado a identificar los RIM tanto en los estados financieros como en las afirmaciones.[43]

La identificación de los RIM se debe realizar antes de considerar cualquier control relacionado, es decir, en primer lugar, se debe identificar el riesgo inherente[44] 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.

46. **El auditor determinará las afirmaciones relevantes y los correspondientes TTSCIR significativos.**[45]

Las **afirmaciones relevantes** tienen por objeto centrar a los auditores en esas afirmaciones para un TTSCIR, en relación con las cuales la naturaleza o las circunstancias son tales 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.

Por definición, **un TTSCIRS es aquel en el que hay una o más afirmaciones relevantes**. Determinar tipos de transacciones, saldos contables e información a revelar ayuda a aclarar el trabajo del auditor en relación con el conocimiento del sistema de información, así como el desarrollo de las respuestas del auditor que son requeridas por la NIA-ES-SP 1330. Con respecto a la información a revelar, el material de aplicación en el párrafo A204 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 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. **El auditor no debe dedicar esfuerzo en aquellas áreas en las que no existe un RIM/afirmación relevante/TTSCIRS.**

Valoración de riesgos de incorrección material en los estados financieros *(párrafo 30 de la NIA-ES 315R)*

47. **La valoración de los RIM identificados en los estados financieros tiene una doble finalidad:**

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).

La NIA-ES 315R hace mayor hincapié en los riesgos en los estados financieros y explica mejor 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[46].

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[47].

[43] Apartado 28 de la NIA-ES 315R.
[44] Apartado A186
[45] Apartado 29 de la NIA-ES 315R.
[46] Apartado A197
[47] Apartado A200 de la NIA-ES 315R.

Valoración de riesgos de incorrección material en las afirmaciones *(párrafos 31 a 34 de la NIA-ES 315R)*

Valoración del riesgo inherente

48. **Para los RIM identificados en las afirmaciones, el auditor valorará el riesgo inherente valorando 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[48]:**

    a. los factores de riesgo inherente 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.

    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.

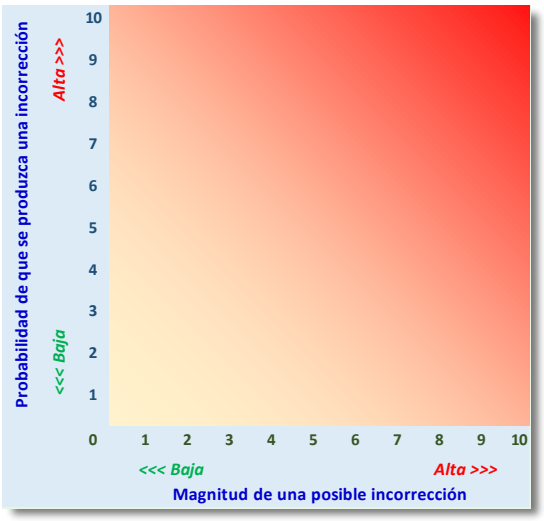
    El enfoque para valorar el riesgo inherente en las afirmaciones es más detallado que los requerimientos de la versión anterior de la norma y se pretende facilitar una mayor coherencia en la valoración de los RIM.

El espectro de riesgo inherente y los riesgos significativos

49. 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. El juicio acerca de la valoración del punto del rango de riesgo inherente en el que se encuentra el riesgo 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.[49]

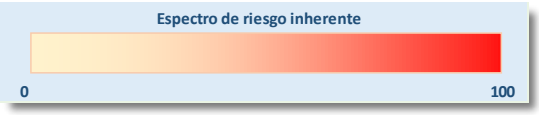
    Es decir, se requiere que se evalúe la combinación de la probabilidad de que ocurra una incorrección material y la magnitud de la posible incorrección para determinar en qué punto del espectro de riesgo inherente valora que se sitúa el riesgo inherente. Cuanto mayor sea la combinación de la probabilidad de que exista y la magnitud, mayor será la valoración del riesgo inherente; cuanto menor sea la combinación de probabilidad y magnitud, menor será la valoración del riesgo inherente.[50]



[48] Apartado 31 de la NIA-ES 315R.
[49] Apartado 209 de la NIA-ES 315R.
[50] Apartados A208-209 de la NIA-ES 315R.

Para visualizarlo se puede utilizar como ejemplo un gráfico como el anterior, 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):

El grado en que varía el riesgo inherente es el espectro del riesgo inherente.[51]



La valoración de los **riesgos inherentes** de esta manera ayuda al auditor 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 utilizados por los auditores.

Por razones prácticas resulta conveniente realizar esta categorización. En la anteriormente vigente GPF-OCEX 1317 se establecían 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 utiliza el **juicio profesional** para determinar la importancia de la combinación de la probabilidad y magnitud de una incorrección. Para que un riesgo valorado sea mayor en el espectro del riesgo inherente, no es necesario que tanto la magnitud como la probabilidad se valoren como altas; la intersección de la magnitud y la probabilidad determinará si el riesgo valorado es mayor o menor en el espectro de riesgo inherente.

50. **El auditor determinará si alguno de los riesgos de incorrección material valorados es un riesgo significativo**[52]**.**

Se redefine de forma más precisa qué debe entenderse por "riesgo significativo", que es uno de los elementos centrales del enfoque de riesgo.

En la anterior NIA-ES 315 se definía, escuetamente, el riesgo significativo como aquel que "*a juicio del auditor, requiere una consideración especial en la auditoría*". Un estudio[53] realizado por IAASB (IAASB 2013) reveló que probablemente esta definición no era clara y que se basaba en un razonamiento circular ya que se centraba en las consecuencias del riesgo más que en la naturaleza del riesgo mismo.

En la nueva NIA-ES 315R, de forma más explícita, se indica que **un riesgo significativo es un riesgo identificado de incorrección material** para el que[54]:

(a) 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

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

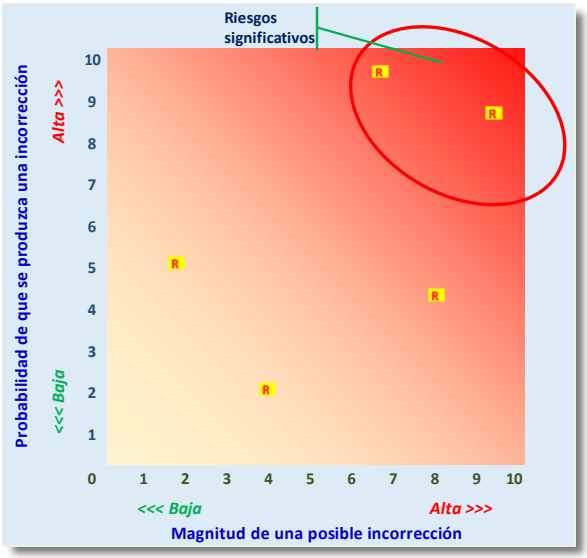
La combinación de probabilidad y magnitud significa que un riesgo significativo podría tener una probabilidad baja, pero la magnitud podría ser muy alta si se produjera. Aunque estos riesgos se consideran menos propensos a ser un riesgo significativo (en comparación con los riesgos en los que tanto la probabilidad como la magnitud son altas), no se han excluido explícitamente

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 requeridas por las NIA-ES[55].

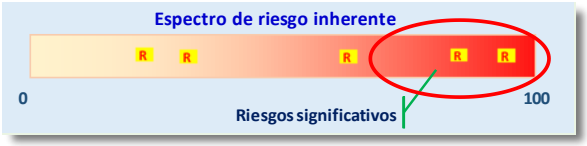
[51] Ver apartado 5 de la NIA-ES 315R.
[52] Apartado 32 de la NIA-ES 315R.
[53] The Clarified ISAs—Findings from the Post-Implementation Review.
[54] Apartado 12.l de la NIA-ES 315R.
[55] Apartado 218 a 221 de la NIA-ES 315R.

En la determinación de los riesgos significativos, el auditor identificará en primer lugar los RIM valorados cuyo riesgo inherente se haya valorado como más alto dentro del espectro de riesgo inherente para sustentar su consideración de qué riesgos se pueden encontrar próximos al límite superior. 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 ofrece algunos ejemplos de cuestiones en las que los riesgos significativos pueden ser más frecuentes.

Podemos visualizarlo con un ejemplo: en una auditoría se han identificado cinco riesgos en las afirmaciones (R) 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:



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

51. **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 valorados de incorrección material en las afirmaciones.**

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 control** por las implicaciones para el diseño y aplicación de procedimientos posteriores de auditoría de conformidad con la NIA 330 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.

Valoración del riesgo de control

52. Si bien **siempre** se está obligado a valorar el riesgo inherente de los riesgos identificados a nivel de afirmación, **solo** se le 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[56].

Si 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 y se haya realizado el trabajo que se exige en los apartados 21 a 27 de la NIA-ES 315R, no es necesario realizar pruebas de los controles.

Existe un vínculo estrecho entre la valoración del riesgo de control y el trabajo realizado para obtener un conocimiento de los componentes del sistema de control interno de la entidad. El conocimiento por parte del auditor del sistema de control interno de la entidad informa las expectativas del auditor sobre la eficacia operativa de los controles y si el auditor planea probar la eficacia operativa de los controles, ayuda 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.

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

53. **Si el auditor planea probar la eficacia operativa de un control de procesamiento de la información (CPI) automatizado, será necesario probar la eficacia operativa de los CGTI relacionados que sustentan su funcionamiento continuo y eficaz[57]**.

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

54. **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.

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

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

Para mejorar la integridad del 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 del apartado 18 de la NIA-ES-SP 1330, los TTSCIRS son materiales si podría 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.

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

[57] Apartados 26, A150 y A229 de la NIA-ES 315R.

En estos casos, la NIA-ES-SP 1330, apartado 18, requiere que, con independencia de los riesgos valorados de incorrección material, el auditor diseñará y aplicará procedimientos sustantivos para cada TTSCIR que resulte material.

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

56. **Si 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.**

V La NIA-ES 315 (Revisada) y la auditoría pública en un entorno de administración electrónica avanzada

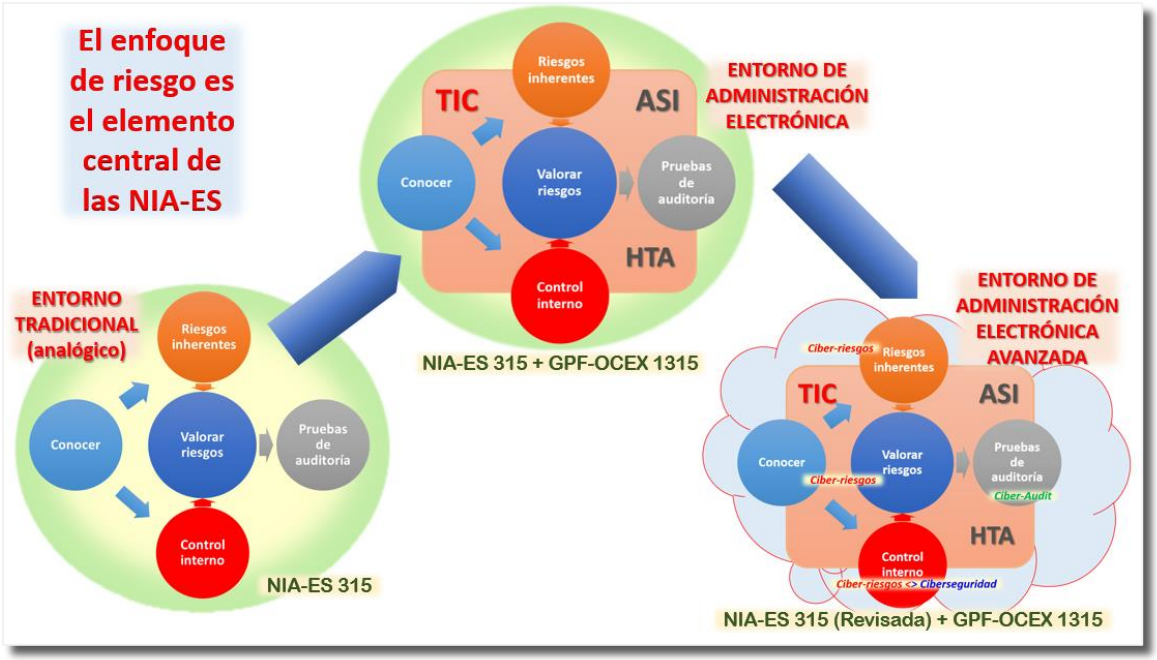
Nuevo entorno digital

57. Los principales rasgos que caracterizan la gestión de las actuales administraciones y entidades públicas son:

- Gestión totalmente digital con ausencia de papel físico.
- Uso intensivo de aplicaciones informáticas complejas, integradas e interconectadas a través de internet.
- Integración de controles internos automatizados o semiautomatizados en las aplicaciones.
- Bases de datos masivas.
- Uso creciente de la computación en la nube y el IoT
- Riesgos crecientes y preocupación por la ciberseguridad.
- Uso creciente de la inteligencia artificial.

Aunque el enfoque de riesgo de la auditoría no ha cambiado básicamente en los últimos 20 años, sí que ha cambiado radicalmente el uso que las entidades públicas realizan de la tecnología, por tanto, los diferentes riesgos derivados del uso de TI también han experimentado un incremento exponencial y, en consecuencia, la forma de abordar por parte de los auditores las auditorías en entornos de AEA también ha evolucionado de forma importante.

La siguiente imagen es una representación simplificada de esta evolución:



La nueva ***NIA-ES 220 (Revisada) Gestión de la calidad de una auditoría de estados financieros***[58] señala que "*la utilización de* ***recursos tecnológicos*** *en una auditoría* ***puede ayudar al auditor en la obtención de evidencia de auditoría suficiente y adecuada****. Las herramientas tecnológicas pueden permitir que el auditor gestione la auditoría de un modo* ***más eficaz y eficiente****.* ***Las herramientas tecnológicas también pueden permitir que el auditor evalúe grandes cantidades de datos con más facilidad para, por ejemplo, proporcionarle información con mayor profundidad, identificar tendencias inusuales o cuestionar más eficazmente las afirmaciones de la dirección, lo que mejora la capacidad del auditor para aplicar el escepticismo profesional.*** *Las herramientas tecnológicas también se pueden utilizar para realizar reuniones y proporcionar* ***herramientas de comunicación*** *al equipo de auditoría. La* ***utilización inadecuada*** *de esos recursos tecnológicos puede, sin embargo, incrementar el* ***riesgo de un exceso de confianza*** *en la información generada para la toma de decisiones, o puede originar amenazas para el cumplimiento de los requerimientos de ética aplicables, por ejemplo, de los requerimientos relacionados con la* ***confidencialidad***".

58. La NIA-ES 315R está pensada y desarrollada para auditar en los actuales entornos de administración electrónica avanzados, en los que toda la gestión y administración es digital, no analógica, sin papel, y contempla expresamente en su texto que el auditado utilice aplicaciones informáticas de gestión integradas (ERP), interconectadas a través de las redes de comunicaciones y con interfaces automáticas, con controles muchas veces automatizados, operando en cloud computing, sujetas a ciberataques crecientes en número y complejidad, con bases de datos masivas, utilizando tecnologías emergentes como el blokchain y la inteligencia artificial, etc. Consecuentemente dedica una porción importante de su contenido a establecer los procedimientos de auditoría, para identificar y valorar riesgos derivados de la utilización de TI, que debe aplicar el auditor en esos entornos digitales, con numerosas orientaciones y ejemplos.

Por tanto, el auditor apoyándose en la NIA-ES 315R debe adaptar su metodología al nuevo entorno de trabajo y a los recursos tecnológicos que tiene a su disposición.

La NIA-ES 315R ha cambiado sustancialmente y mejorado los requerimientos y el material de aplicación en relación con las consideraciones que debe realizar el auditor sobre TI respecto de la anterior NIA-ES 315. El párrafo A170 de NIA-ES 315R explica que **la amplitud del conocimiento del auditor de los procesos de TI, incluido el grado en que la entidad ha establecido controles generales de TI, variará según la naturaleza y las circunstancias de la entidad y de su entorno de TI, así como según la naturaleza y extensión de los controles identificados por el auditor.**

Algunos cambios con respecto a las TI se recogen ya en las nuevas definiciones:

Nuevas definiciones	Descripción	Material explicativo adicional
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 la NIA-ES 315R: (i) 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. (ii) La **infraestructura de TI** comprende la red, los sistemas operativos y las bases de datos y el hardware y software relacionados con estos. (iii) Los **procesos de TI** son los procesos de la entidad para la gestión del acceso al entorno de TI, la gestión de cambios en los programas o de los cambios al entorno de TI, así como para la gestión de las operaciones de TI.	N/A

[58] Apartado A63 de la NIA-ES 220 (Revisada) (ver Resolución de 2 de febrero de 2022, del ICAC).

Nuevas definiciones	Descripción	Material explicativo adicional
Riesgos derivados de la utilización de TI	**Exposición de los CPI 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.**	Los riesgos para la integridad de la información se originan por la susceptibilidad a una implementación ineficaz de las políticas de información de la entidad, que son políticas que definen los flujos de información, los registros y los procesos de información del sistema de información de la entidad. (A6)

En el ***Anexo 5 Consideraciones para el conocimiento de las tecnologías de la información*** se proporcionan cuestiones adicionales que el auditor puede considerar para el conocimiento de la utilización de las TI en el sistema de control interno, incluyendo:

- Aspectos a tener en cuenta al conocer el uso de TI por parte de la entidad en los componentes del sistema de control interno.
- Ejemplos de características típicas de sistemas de información con diferentes complejidades.
- Consideraciones sobre tecnologías emergentes.
- Consideraciones en torno a la graduación.
- Material de apoyo para la identificación de aplicaciones TI que están sujetas a riesgos derivados del uso de TI.
- Otros aspectos del entorno de TI sujetos a riesgos derivados de la utilización de TI.
- Orientaciones sobre los casos en que puede haber un mayor riesgo relacionado con la ciberseguridad.
- Identificación de riesgos derivados de la utilización de TI y CGTI

Conocimiento de los riesgos de negocio derivados del uso de las tecnologías de la información

59. La NIA-ES 315R **requiere que los auditores obtengan un conocimiento de la entidad y su entorno, que incluya el modelo de negocio de la entidad y el modo en que ese modelo de negocio integra la utilización de TI en sus interacciones con clientes/usuarios/contribuyentes, proveedores, fuentes de financiación y otros interesados mediante intercomunicaciones de TI y otras tecnologías[59].**

Conocer el modelo de negocio y el uso de TI ayuda al auditor a entender los riesgos de negocio a los que se enfrenta una entidad, pero no todos los riesgos de negocio dan lugar a riesgos de incorrección material en las cuentas anuales.

En la nueva NIA-ES 315R se definen los **riesgos derivados de la utilización de TI** como:

- **la exposición de los CPI 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.**

Los procesos de negocio se basan, en general, en sistemas automatizados para soportar procesos eficientes y efectivos, así como los controles. Como resultado, **los riesgos de TI son parte integral, no separados, de los riesgos del negocio**.

Cuando el auditor identifica aplicaciones informáticas que están sujetas a riesgos derivados del uso de TI, existen otros aspectos del entorno TI que también suelen estar sujetos a riesgos derivados del uso de TI. Como se señaló anteriormente, los otros aspectos del entorno de TI incluyen bases de datos, sistemas operativos y redes. Así, algunos *ejemplos* de riesgos derivados del uso de TI en el entorno TI incluyen:

- *Bases de datos*: se puede acceder directamente a una base de datos que almacena los datos relacionados con la preparación de los estados financieros.

[59] Véase el párrafo 19 y el Anexo 1 de la NIA-ES 315R

- *Sistema operativo*: El sistema operativo a través del cual se accede a las aplicaciones y bases de datos pertinentes para la preparación los estados financieros puede estar sujeto a riesgos derivados de TI cuando no se gestionan adecuadamente los accesos.

Aunque los riesgos relacionados con TI, incluidos los de ciberseguridad, son un riesgo para cualquier entidad, no todas las entidades se pueden ver afectadas de la misma manera. Estos riesgos no siempre dan lugar a un RIM en las cuentas anuales que exija que el auditor diseñe y aplique una respuesta (un procedimiento de auditoría posterior). Dependerá de su modelo de negocio y cómo se utilizan las TI. *Por ejemplo*, en una entidad de gestión tributaria cuya gestión se realiza apoyándose totalmente en complejos sistemas y aplicaciones informáticas alojadas en la *nube*, el riesgo de negocio derivado del uso de TI y de ciberseguridad sería crítico. Sin embargo, para un consorcio de bomberos el riesgo de negocio derivado del uso de TI y de ciberseguridad sería más bajo. Por tanto, vemos como la valoración del riesgo inherente derivado de la actividad de la entidad auditada, del uso de TI y de la ciberseguridad puede ser muy distinto.

Conocimiento de la utilización de TI en los componentes del sistema de control interno de la entidad

60. El apartado A94 de la NIA-ES 315R 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**.

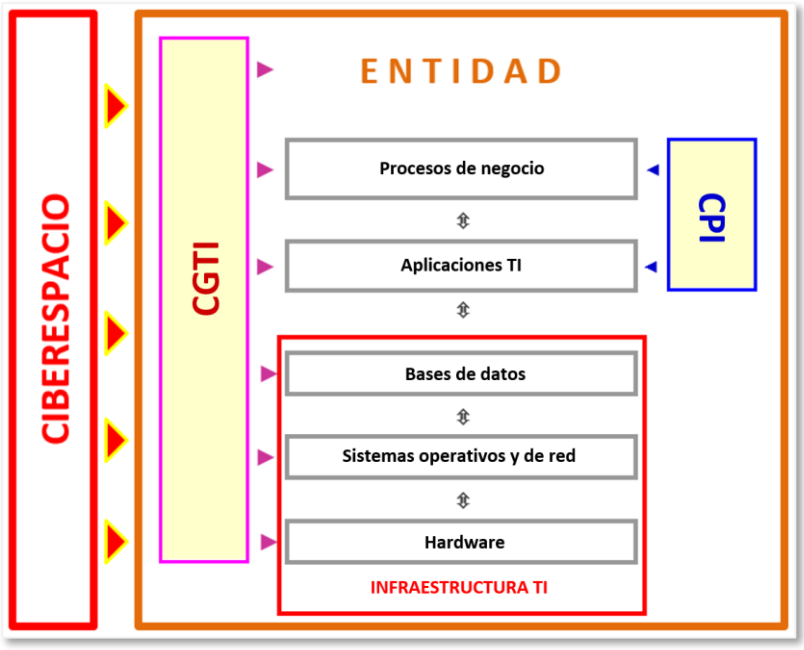
Aunque el objetivo y el alcance de una auditoría no sean diferentes, el grado de digitalización de la entidad, además de a los riesgos inherentes, afecta a la forma en que debe realizarse el conocimiento del sistema de control interno y de sus componentes, a la valoración de los riesgos de control y al tipo de pruebas que se pueden realizar de los controles automatizados.

Algunas consideraciones sobre los componentes de un sistema de control interno y su relación con las TI:

- La evaluación por el auditor del **entorno de control**[60] en relación con la utilización de TI por la entidad incluirá cuestiones tales como si la **gobernanza sobre las TI**[61] es acorde con la naturaleza y complejidad de la entidad y de las operaciones de negocio realizadas a través de TI, incluida la complejidad o madurez de la plataforma o arquitectura tecnológicas de la entidad y hasta qué punto confía la entidad en aplicaciones de TI para sustentar su información financiera.
- El auditor también debe considerar el modo en que el **proceso de la entidad para el seguimiento del sistema de control interno**[62] en el que interviene la utilización de TI realiza el seguimiento de los CPI (anteriormente denominados controles de aplicación). Esto puede incluir, por ejemplo: controles para el seguimiento de entornos de TI complejos o controles de segregación de funciones.
- El conocimiento que debe adquirir el auditor del **sistema de información**[63] incluye el entorno de TI relevante para los flujos de transacciones y el procesamiento de la información porque la utilización de aplicaciones de TI u otros aspectos del entorno de TI pueden dar lugar a riesgos derivados de la utilización de TI.
- Las **actividades de control**. La NIA-ES 315R dedica un amplísimo espacio a las consideraciones que el auditor debe realizar sobre el conocimiento, identificación y valoración de riesgos, y la identificación y evaluación de controles automatizados en un entorno TI.

[60] Apartado A108 de la NIA-ES 315R.
[61] Véase la GPF-OCEX 5331 Gobernanza corporativa, gobernanza sobre las TI y su auditoría.
[62] Apartado A117 de la NIA-ES 315R.
[63] Apartado A140 de la NIA-ES 315R.

El siguiente gráfico muestra de forma simplificada un esquema de un sistema de información/entorno TI:



Los controles generales de TI (CGTI)

Qué son los CGTI

61. Los CGTI son las políticas y procedimientos que se aplican a la totalidad o a gran parte de los sistemas de información de una entidad, incluyendo la infraestructura y plataformas TI de la organización auditada y ayudan a asegurar su correcto funcionamiento. Son controles relacionados con el uso de las tecnologías de la información y las comunicaciones implantados en los distintos niveles de la estructura organizativa general de una institución y en sus sistemas de información.

El apartado 26 de la NIA-ES 315R requiere que el auditor identifique y evalúe los CGTI para aplicaciones TI y otros aspectos del entorno TI que el auditor haya determinado que están sujetos a riesgos derivados de la utilización de TI porque los CGTI sustentan el funcionamiento continuo y eficaz de los CPI.[64]

Hay que destacar que el auditor **no** es responsable de conocer todos los CGTI existentes en el entorno TI y realizar las pruebas subsiguientes. La responsabilidad del auditor se limita a los CGTI que tienen una relación directa con la preparación de los estados financieros.

Cuanto mayor sea la extensión de los controles automatizados, o de los controles en los que participa algún proceso automatizado, que utilice la dirección y en los que confíe en relación con su información financiera, más importante puede llegar a ser para la entidad implementar CGTI que traten el funcionamiento continuo de los aspectos automatizados de los CPI[65].

Desde el punto de vista del auditor del sector público, los objetivos de los CGTI son proporcionar una garantía razonable de que los datos, la información y los activos de los SI cumplen las siguientes propiedades, que coinciden con las cinco dimensiones de la seguridad de la información que establece el ENS, que es de obligado cumplimiento en el sector público:

[64] Apartado A150 de la NIA-ES 315R.

[65] Apartado 20 del Anexo 2 de la NIA-ES 315R.

Objetivos de los CGTI	Descripción (según la GPF-OCEX 5330)
Confidencialidad	Es la propiedad de la información por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.
Integridad	Es la propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales. ***Según la NIA-ES 315R esta propiedad incluye la completitud, exactitud y validez de la información.***
Disponibilidad	Se trata de la capacidad de un servicio, un sistema o una información, de ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.
Autenticidad	Es la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
Trazabilidad	Es la propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Unos CGTI sólidos constituyen una buena línea de defensa para la ciberseguridad.

La **finalidad** de los CGTI en un entorno informatizado es establecer un marco general de control y confianza sobre las actividades del sistema informático y asegurar razonablemente la consecución de los objetivos generales de control interno y el correcto funcionamiento de los CPI.

Su importancia radica en que tienen un **efecto generalizado**, es decir, suelen afectar a más de una aplicación informática, y si los CGTI no funcionan adecuadamente se imposibilita que se pueda confiar en los CPI.

Porqué se deben auditar

62. Para cada uno de los CGTI identificados se evaluará si está diseñado eficazmente para sustentar el funcionamiento de otros controles y determinará si el control ha sido implementado eficazmente.

    Los auditores responsables de cada auditoría deben analizar cómo afectan las cuestiones relacionadas con la seguridad informática y la ciberseguridad a los objetivos de la auditoría. Cuanto mayor sea la entidad auditada y más complejos sus sistemas de información, mayor impacto tendrán los aspectos tecnológicos y los riesgos TI, y mayores serán las consideraciones al respecto que deba hacerse el auditor.

    Tal como se ha señalado antes, **si el auditor planea probar la eficacia operativa de un control de procesamiento de la información (CPI) automatizado, será necesario probar la eficacia operativa de los CGTI relacionados que sustentan su funcionamiento continuo y eficaz**[66].

Cuáles son

63. De acuerdo con la metodología establecida en la GPF-OCEX 5330, la revisión de los CGTI se estructura en las cinco áreas siguientes:

    A. Marco organizativo *(entorno de control)*
    B. Gestión de cambios en aplicaciones y sistemas
    C. Operaciones de los sistemas de información
    D. Controles de acceso a datos y programas
    E. Continuidad del servicio

64. Para identificar los CGTI, la guía de aplicación de la NIA-ES 315R:

    (a) Explica que los controles identificados por el auditor pueden depender de informes generados por el sistema, en cuyo caso las aplicaciones que producen dichos informes pueden estar sujetas a riesgos derivados del uso de TI.

        El auditor puede planear no confiar en los controles de los informes generados por los sistemas y, más bien, planea probar directamente las entradas y salidas de dichos informes, en cuyo caso el auditor

[66] Apartados 26, A150 y A229 de la NIA-ES 315R.

puede no identificar las aplicaciones TI relacionadas como sujetas a riesgos derivados del uso de TI.

(b) Deja claro que la extensión del conocimiento de los procesos de TI variará con la naturaleza y las circunstancias de la entidad y su entorno informático (véase el párrafo A170 y los ejemplos)

(c) Explica cuándo pueden ser relevantes los demás aspectos del entorno informático sujetos a riesgos derivados del uso de TI que incluyen la red, los sistemas operativos y bases de datos y, en determinadas circunstancias, las comunicaciones (interfaces) entre aplicaciones de TI (véase el párrafo A172).

(d) Explica que la identificación de los riesgos derivados del uso de TI se refiere únicamente a las aplicaciones TI identificadas de acuerdo con lo que se indica en el apartado 26, letra b), de la NIA-ES 315R (véanse los ejemplos del material de aplicación en los apartados A173 a 174 de la NIA-ES 315R).

En el ***Anexo 6 Consideraciones para el conocimiento de los CGTI*** de la NIA-ES 315R se proporcionan consideraciones adicionales para que el auditor tenga en cuenta en el conocimiento de los CGTI.

¿Cuándo se debe probar su eficacia operativa?

65. De conformidad con la letra d) del párrafo 26 de la NIA-ES 315R, el auditor deberá evaluar, para cada uno de los controles identificados en los apartados 26, letras a) y c), si el control está diseñado de manera eficaz para hacer frente al RIM en las afirmaciones, o bien diseñado para apoyar el funcionamiento de otros controles y determinar si se ha implementado (D+I). Esto ocurre independientemente de si el auditor planea confiar en la eficacia operativa de los controles como parte de su respuesta planificada para abordar los RIM valorados.

Cuando el auditor planea confiar en la eficacia operativa de los controles como parte de su respuesta para abordar los RIM valorados y esos controles dependen de los CGTI, el auditor deberá probar la eficacia operativa de los CGTI (NIA-ES-SP 1330, ap10).

Si bien la razón más común por la que se prueba la eficacia operativa de un CGTI es apoyar la evaluación por parte del auditor de la eficacia operativa de un CPI automatizado, puede haber otros casos en los que las pruebas sobre la eficacia operativa de los CGTI sean pertinentes para otros procedimientos, que pueden incluir:

- Procedimientos analíticos sustantivos: los CGTI pueden ser pertinentes cuando el auditor está probando la fiabilidad de los datos que se utilizarán en un procedimiento analítico sustantivo y ha determinado que esto se hará mediante la prueba de la eficacia operativa de los CPI. En esta situación, el auditor confía en la eficacia operativa de los CPI para proporcionar evidencia sobre la completitud, exactitud y validez de los datos que forman parte de los procedimientos analíticos sustantivos del auditor. (Por ejemplo, tasas unitarias de una lista maestra que se utilizarán para recalcular el valor de una determinada clase de transacciones).
- Controles sobre los asientos de diario: el auditor puede confiar en los CGTI que administran los permisos para registrar los asientos de diario no estándar y se deberán comprobar.
- Informes personalizados: cuando los procedimientos sustantivos del auditor utilizan informes generados por el sistema, el auditor probará la eficacia operativa de los CGTI que abordan el riesgo de cambios inapropiados, no autorizados o directos en el informe.

Las herramientas y técnicas automatizadas (HTA)

66. Debido a la creciente e imparable utilización de herramientas y técnicas automatizadas en la realización de procedimientos de auditoría, la NIA-ES 315R trata diferentes aspectos de su uso en varios apartados específicos titulados "Herramientas y técnicas automatizadas".

Siguen siendo aplicables los procedimientos de obtención de evidencia de auditoría establecidos en la *NIA-ES-SP 1500, Evidencia de auditoría*, es decir, inspección, observación, confirmación externa, recálculo, reejecución, procedimientos analíticos e indagación, independientemente de que dichos procedimientos se realicen manualmente o utilizando tecnología. La NIA-ES 315R no es prescriptiva en cuanto a cómo se deben realizar estos procedimientos. También debe consultarse la *GPF-OCEX 1503 Evidencia electrónica*.

Adicionalmente, dada la importancia que está adquiriendo en la actividad auditora la utilización de HTA, la IAASB ha emitido una serie de guías orientativas (IAASB Technology FAQ) sobre su utilización por el auditor en el marco de las NIA.

Sobre esta materia se recomienda la lectura de la **GPF-OCEX-5370 Guía para la realización de pruebas de datos**.

67. Los procedimientos de auditoría pueden llevarse a cabo utilizando una serie de herramientas[67] o técnicas[68], que pueden ser manuales o automatizadas o una combinación de ambas.

A los efectos de una auditoría, las HTA consisten en el uso de herramientas TI para llevar a cabo procedimientos de auditoría, lo que conlleva la automatización de estos.

En ciertas circunstancias, un auditor puede considerar que el uso de HTA para llevar a cabo determinados procedimientos puede dar lugar a evidencias de auditoría más convincentes en relación con la afirmación que se está comprobando (*por ejemplo, cuando se audite una entidad grande que opera en un entorno de administración electrónica avanzada*). En otras circunstancias, la realización de procedimientos de auditoría puede ser eficaz sin el uso de HTA e incluso resultar más apropiado, en términos de eficiencia, no utilizarlas (*por ejemplo, cuando se audite una entidad pequeña, con poco personal y procesos sencillos y manuales*).

Al aplicar las NIA-ES-SP, un auditor puede diseñar y realizar procedimientos de auditoría manualmente o mediante el uso de HTA, y cualquier técnica puede ser eficaz. **Independientemente de las herramientas y técnicas utilizadas, el auditor debe cumplir con las NIA-ES-SP**.

Los auditores pueden utilizar HTA en un procedimiento de auditoría para procesar, organizar, estructurar o presentar datos a fin de generar información que pueda utilizarse como evidencia de auditoría, tanto en los procedimientos de valoración de riesgos como en los procedimientos de auditoría posteriores.

Fuente: GPF-OCEX 5370 Guía para la realización de pruebas de datos

68. Las HTA engloban procedimientos y técnicas de distinta naturaleza, incluido el análisis de datos mediante modelización y visualización, automatización de procesos robóticos, inteligencia artificial y aprendizaje automático, y tecnología de drones para observar o inspeccionar activos[69]. El uso de tales herramientas y técnicas automatizadas puede complementar o reemplazar tareas manuales o repetitivas.

Entre los **tipos de herramientas y técnicas automatizadas** que pueden utilizarse para llevar a cabo los procedimientos de auditoría cabe citar los siguientes:

- **Análisis de datos (ADA)[70]**: utilizados para evaluar conjuntos completos de datos mediante el descubrimiento y análisis de patrones y tendencias, la identificación e investigación de elementos inusuales, desviaciones y anomalías. También puede utilizarse para la identificación y valoración de riesgos de incorrección material que pueden no haber sido tan fácilmente visibles o evidentes mediante el uso de procedimientos más tradicionales. Dentro de este apartado estarían las técnicas de visualización (*A31*) y las técnicas de minería de procesos (*A57 y A137*).

[67] Las **herramientas** son el *software* que permite realizar los tratamientos de los datos precisos para ejecutar las pruebas de auditoría. Por ejemplo, Excel, Access, Power BI, Power Pivot, ACL, IDEA, Tableau, SAS, etc.

[68] **Técnicas** son las diferentes formas en que se accede, se organizan, se analizan los datos y se comunican los resultados.

[69] NIA-ES 315 (revisada), apartado A35.

[70] NIA-ES 315 (revisada), apartado A31.

- **Automatización robótica de procesos (RPA)**: consiste en el procesamiento de datos estructurados mediante un software que automatiza las actividades que los seres humanos realizan, tareas típicamente repetitivas que requieren un juicio mínimo. *Por ejemplo, la RPA se puede utilizar para realizar el análisis del libro mayor general e identificar asientos que no cuadran, están duplicados, están por encima de un umbral definido o muestran ciertas características o para automatizar la carga de datos, verificar su integridad y ejecutar pruebas estándar, como muestreos.*
- **Técnicas de inteligencia artificial**: tecnología de aprendizaje automático configurada para reconocer patrones en grandes volúmenes de datos, incluidos datos no estructurados como correos electrónicos, contratos, facturas, imágenes y archivos de audio de reuniones. Los auditores pueden utilizar la inteligencia artificial para reunir información de diversas fuentes y determinar los riesgos de incorrecciones materiales.

La ciberseguridad

69. Si los **riesgos de ciberseguridad** son una parte de los riesgos derivados de la utilización de TI[71] por parte de una entidad, los controles de ciberseguridad son un subconjunto significativo de los CGTI orientados a protegerla frente a ese tipo de amenazas. En la medida que una entidad está más interconectada con el exterior y sus sistemas son más complejos, las amenazas y los riesgos aumentan y es necesario implantar controles de seguridad más estrictos. Esto incluye todo lo relacionado con la ciberseguridad.

    Uno de los aspectos a conocer es la **gobernanza de la ciberseguridad[72]**, que es un componente esencial de la gobernanza TI, más relevante cuanto más interconectados estén los sistemas de información de la entidad auditada. Es importante tanto desde un punto de vista del riesgo Ti y del control interno como del cumplimiento legal en una entidad pública.

    Todo este escenario debe ser conocido por el auditor, que tiene a su disposición las GPF-OCEX 5311, 5313 y 5314.

Cloud computing: Consideraciones generales que deben realizarse en una auditoría financiera

70. La nueva NIA-ES 315R señala en varios de sus apartados, en especial en el Anexo 5 distintas cuestiones relacionadas con la utilización de la computación en la nube que debe tener en cuenta el auditor.

    Un auditor debe, como parte esencial de sus procedimientos de auditoría financiera, conocer el sistema de información y de control interno de la entidad auditada, identificar y valorar riesgos, incluidos los derivados de la utilización de las TI, identificar y revisar los controles incluyendo los automatizados y diseñar y ejecutar las pruebas pertinentes adaptadas a las circunstancias particulares.

    Una de las primeras fases de una auditoría es adquirir un conocimiento de los riesgos de negocio derivados del uso de las tecnologías de la información. En la medida que algunas de las áreas significativas para la auditoría (por ejemplo, la gestión tributaria en un ayuntamiento, las nóminas o la gestión económica y contable en una entidad) se gestionen mediante aplicaciones en la nube, el auditor deberá conocer cómo se han desplegado las aplicaciones y adaptar convenientemente sus procedimientos para tener en cuenta las características y riesgos específicos de ese entorno tecnológico. Un entorno cloud no es sino una particularidad de un entorno TI, con sus características y riesgos específicos que en todo caso se debe conocer así como los controles internos.

    De acuerdo con el enfoque de riesgo y lo previsto en la NIA-ES 315R, el auditor deberá tener en cuenta en cada etapa de la auditoría el efecto sobre su trabajo del hecho de que una parte significativa de la gestión del ente auditado esté soportada mediante sistemas TI y, si fuera el caso, mediante el procesamiento en la nube.

71. Por otra parte, los servicios de computación en la nube o cloud computing solo son un caso particular de los servicios contemplados en la *NIA-ES-SP 1402 "Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios"*. En 2020 la Conferencia de Presidentes de los OCEX aprobó la Guía Práctica de Fiscalización de los Órganos de Control Externo *GPF-OCEX 1403 Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios de computación en la nube.* Su finalidad es orientar sobre cómo se debe aplicar la *NIA-ES-SP 1402* cuando el ente que vamos a fiscalizar utiliza servicios

[71] Ver apartado A174 y el anexo 5.

[72] Véase la GPF-OCEX 5314 Gobernanza de la ciberseguridad y su auditoría.

de computación en la nube.

La NIA-ES-SP 1402 y la GPF-OCEX 1403 se aplican cuando una entidad auditada (usuaria) recibe servicios de cloud computing de otra entidad (organización de servicios o entidad prestadora o CSP) relacionados con aquellas áreas de la entidad (contabilidad, compras, personal, ingresos, etc) en las cuales el auditor tiene que valorar el riesgo, aplicar procedimientos de auditoría, revisar el sistema de control interno y obtener evidencia de auditoría, que es lo que requiere la NIA-ES 315R y la NIA-ES-SP/GPF-OCEX 1330.

El objetivo de una auditoría financiera no varía por el hecho de que una entidad tenga varios servicios y aplicaciones significativas operando en la nube mediante un contrato de servicios.

La necesidad de contar con auditores de sistemas de información en los equipos de auditoría

72. La NIA-ES 315R señala en el párrafo A55 que "***la utilización de TI y la naturaleza y extensión de cambios en el entorno de las TI pueden afectar también a las cualificaciones especializadas necesarias para ayudar en la obtención del conocimiento requerido***" de la entidad, de su entorno TI y del sistema de control interno. Y en el párrafo A171 se insiste en que "***cuando el entorno de TI de una entidad es más complejo, es probable que la identificación de las aplicaciones de TI y otros aspectos del entorno de TI, la determinación de los riesgos relacionados derivados de la utilización de TI y la identificación de controles generales de TI requiera la participación de miembros del equipo con cualificaciones especializadas en TI. Es posible que esa participación sea esencial y tenga que ser extensa en el caso de entornos de TI complejos***", como son los entornos de administración electrónica avanzada.

De acuerdo con esto, **para auditar entidades medianas o grandes operando en un entorno de administración electrónica avanzada deben formarse equipos mixtos, integrados por auditores financieros y por especialistas en auditoría de sistemas de información y ciberseguridad, trabajando conjuntamente con metodología actualizada basada en las NIA-ES/NIA-ES-SP, en especial en la NIA-ES 315R**, y en las **GPF-OCEX**, de forma que se haga un trabajo adaptado a las nuevas circunstancias mucho más eficaz y eficientemente.

Los expertos en seguridad TI analizarán juntamente con los auditores financieros aquellos riesgos y controles que son relevantes para los objetivos de la auditoría financiera, con un enfoque de riesgo adaptado a las necesidades de los auditores financieros, ya que no todos los riesgos que pretenden mitigar los CGTI son iguales, ni en probabilidad, ni en su materialidad, ni en su importancia para el auditor.

No hacerlo de esta forma, no abordando los riesgos relacionados con la seguridad de la información y la ciberseguridad con personal especializado en TI integrado en los equipos de auditoría, **supone no cumplir con la NIA-ES 315R y asumir unos riesgos de auditoría hasta niveles muy elevados y, en muchos casos, inaceptables.**

Si las plantillas no incorporan auditores de sistemas de información y expertos en ciberseguridad, se dispone del recurso de contratar expertos externos para cubrir ese déficit de conocimientos y de profesionales especializados.

VI Documentación

73. Se requiere documentación adicional a la exigida por la NIA-ES-SP 1230, en particular para documentar los «juicios significativos» que el auditor haga al identificar y valorar los riesgos de incorrección material.

    (a) Los resultados de la discusión entre los miembros del equipo del encargo, así como las decisiones significativas que se tomaron (ver apartado 17 de la GPF-OCEX 1315R y el modelo para su documentación en la GPF-OCEX 1513).

    (b) Elementos clave de la comprensión por el auditor de la entidad y su entorno, el marco de información financiera aplicable y cada uno de los componentes del sistema de control interno de la entidad de conformidad con los apartados 19, 21, 22, 24 y 25 de la GPF-OCEX 1315R. La documentación debe incluir la fuente de la información, así como los procedimientos de valoración de riesgos realizados.

    (c) La evaluación del diseño de los controles identificados y la determinación de si dichos controles han sido implementados, de conformidad con los requerimientos del apartado 26.

(d) Los riesgos de incorrección material en los estados financieros y en las afirmaciones identificados y valorados, incluidos los riesgos significativos y los riesgos para los cuales los procedimientos sustantivos por sí solos no pueden proporcionar evidencia de auditoría suficiente y adecuada, y el fundamento de los juicios significativos aplicados.

(e) El párrafo A238 de la GPF-OCEX 1315R también señala varios asuntos que podrían documentarse para demostrar el ejercicio del escepticismo profesional por parte del auditor.

Es posible que sea necesaria documentación más detallada, que sea suficiente para permitir a un auditor experimentado, que no haya tenido contacto previo con la auditoría, la comprensión de la naturaleza, el momento de realización y la extensión de los procedimientos de auditoría aplicados, para sustentar el fundamento de los juicios difíciles aplicados (apartado A240 de la GPF-OCEX 1315R).

VII Bibliografía

- Australian Auditing and Assurance Standards Board, AUASB Bulletin: ASA 315 and the Auditor's Responsibilities for General IT Controls, junio 2022.
- Chartered Professional Accountants Canada, The Risk Assessment Process: Tips on Implementing Revised CAS 315, junio 2021.
- IAASB, Clarified ISAs, Findings from the post-implementation review, 2013.
- IAASB, Introducción a NIA 315 (Revisada) Identificación y valoración del riesgo de incorrección material, 2019.
- IAASB, Guía de aplicación no obligatoria relativa a la tecnología: La utilización de HTA para la realización de procedimientos de valoración del riesgo de conformidad con la NIA 315 (revisada), 2020
- IAASB, Addressing risk of overreliance on technology arising from the use of automated tools and techniques and from information produced by an entity's systems, 2021.
- IAASB, ISA 315 (Revised 2019), First-Time Implementation Guide, 2022.
- ICAC, NIA-ES 315 (Revisada) Identificación y valoración del riesgo de incorrección material.
- Minguillón Roy, Antonio Novedades de la nueva NIA-ES 315 (Revisada) "Identificación y valoración del riesgo de incorrección material" y su impacto inmediato en la actividad del auditor del sector público en un entorno de administración electrónica avanzada, Serie Opiniones FIASEP, Nº 14/2022 de mayo 2022.
- Rubio Herrera, Enrique, Nueva norma de auditoría sobre identificación y valoración de riesgos de incorrección material (NIA-ES 315Revisada), Técnica Contable y Financiera, nº 55, septiembre de 2022.

VIII Acrónimos utilizados

AEA	Administración electrónica avanzada
ADA	Análisis de datos
ENS	Esquema Nacional de Seguridad
ERP	Aplicaciones informáticas de gestión integradas
CGTI	Controles generales de las tecnologías de la información
GPF-OCEX	Guía práctica de fiscalización de los OCEX
CPI	Controles de procesamiento de la información
HTA	Herramientas y técnicas automatizadas
IAASB	International Auditing and Assurance Standards Board
ICAC	Instituto de Contabilidad y Auditoría de Cuentas
IoT	Internet de las cosas
NIA	Norma internacional de auditoría
PVR	Procedimientos de valoración del riesgo
RIM	Riesgo de incorrección material
RPA	Automatización robótica de procesos

SI	Sistema de información
SIC	Sistema de información y comunicación
TI	Tecnologías de la información
TTSCIR	Tipos de transacciones, saldos contables e información a revelar
TTSCIRS	Tipos de transacciones, saldos contables e información a revelar significativos

Control de versiones

Versión	Cambios
03-11-2022	Versión inicial
19-10-2023	Se subsanan varias erratas y se corrigen ligeramente algunas oraciones para que sea más comprensible el texto, sin alterar el sentido original del documento. También se eliminan algunas reiteraciones. Apartado 5: se elimina del cuadro la definición de RIM, ya que está repetida en el cuadro del apartado 43. Se añaden al cuadro dos definiciones de la NIA-ES-SP 1200 para dejar claros dos conceptos básicos: incorrección e incorrección material. Apartado 7: se corrige un error del gráfico y se cambia de orden el último párrafo. Apartado 14: se sustituye el texto por una imagen. Apartado 18: el último párrafo se pasa al apartado 15, en donde por el contexto se comprende mejor. Apartado 29: se añade un último párrafo para ayudar en la comprensión. Apartado 32: se añade al margen la referencia al apartado en el que se trata el tema en cuestión. Apartado 43: se añaden tres párrafos al final para ayudar en la comprensión. En el cuadro se completa el material explicativo adicional de los RIM con el que había en el cuadro del apartado 5. Apartado 55: se corrigen erratas y se añade un párrafo final. Se han eliminado las notas al pie 3 y 4. El resto se renumera. Nota al pie nº 14: se simplifica. Nota al pie nº 20: se añade para referenciar la nueva GPF-OCEX 5331. Nota al pie nº 21: se añade para referenciar la GPF-OCEX 1512. Nota al pie nº 25: se añade para ayudar en la comprensión. Nota al pie nº 62: se añade para referenciar la nueva GPF-OCEX 5331. Se añade, al final, un apartado de Acrónimos.