Exposición de trabajos en la Cátedra de Tecnología Aplicada a la Información Contable. MCI - Cátedra de Tecnología Aplicada a la Información Contable, Buenos Aires, 2025.

NORMA INTERNACIONAL DE AUDITORIA 315 – IDENTIFICACION Y VALORACION DEL RIESGO DE INCORRECCION MATERIAL DESDE UNA PERSPECTIVA DE TECNOLOGIAS DE LA INFORMACIÓN.

Aoki, Santiago Gabriel y Lavilla Cointte, Agostina.

Cita:

Aoki, Santiago Gabriel y Lavilla Cointte, Agostina (2025). *NORMA INTERNACIONAL DE AUDITORIA 315 – IDENTIFICACION Y VALORACION DEL RIESGO DE INCORRECCION MATERIAL DESDE UNA PERSPECTIVA DE TECNOLOGIAS DE LA INFORMACIÓN. Exposición de trabajos en la Cátedra de Tecnología Aplicada a la Información Contable. MCI - Cátedra de Tecnología Aplicada a la Información Contable, Buenos Aires.*

Dirección estable:
https://www.aacademica.org/mci.catedra.de.tecnologia.aplicada.a.la.informacion.contable/9

ARK: https://n2t.net/ark:/13683/pYAR/Ssm

Universidad de Buenos Aires

Facultad de Ciencias Económicas

Escuela de Estudios de Posgrado

MAESTRIA EN CONTABILIDAD INTERNACIONAL

TECNOLOGIA APLICADA A LA INFORMACION CONTABLE

Tema:

NORMA INTERNACIONAL DE AUDITORIA 315 – IDENTIFICACION Y VALORACION DEL RIESGO DE INCORRECCION MATERIAL DESDE UNA PERSPECTIVA DE TECNOLOGIAS DE LA INFORMACIÓN.

Maestrandos:

- **Aoki, Santiago Gabriel – santiaoki@gmail.com**
- **Lavilla Cointte, Agostina – agostinalavilla@gmail.com**

PRIMER CUATRIMESTRE 2025

En este articulo vamos a tratar sobre la Norma internacional de auditoria 315, esta norma Internacional detalla la responsabilidad del auditor para identificar y valorar los riesgos de incorrección material en los estados financieros. Establece procedimientos y un marco para comprender la entidad, su entorno y controles internos, con el fin de diseñar respuestas de auditoría adecuadas. Distingue entre riesgo inherente y de control, y subraya la importancia del juicio y escepticismo profesional. Desarrollaremos principalmente cómo el auditor debe enfocarse en el análisis de la estructura organizativa, de propiedad y de gobierno de la entidad y su modelo de negocio, incluido el grado de integración en el uso de TI.

Palabras Clave: Riesgo, Incorrección, Auditoría, Control Interno, Afirmaciones, Tecnología de la Información.

1. INTRODUCCION

Esta Norma Internacional de Auditoría (NIA) 315 (Revisada 2019) aborda la responsabilidad del auditor de identificar y valorar el riesgo de incorrección material en los estados financieros. Fue desarrollada y aprobada por el Consejo de Normas Internacionales de Auditoría y Aseguramiento (IAASB), con el apoyo de la Federación Internacional de Contadores (IFAC). Es aplicable a las auditorías de estados financieros correspondientes a periodos iniciados a partir del 15 de diciembre de 2021, y debe interpretarse conjuntamente con la NIA 200, que trata los objetivos globales del auditor independiente.

El objetivo principal del auditor es identificar y valorar los riesgos de incorrección material, ya sea por fraude o error, tanto a nivel de los estados financieros en su conjunto como a nivel de las afirmaciones para las clases de transacciones, saldos contables e información a revelar. Esta valoración es crucial, ya que proporciona el fundamento para el diseño y la implementación de respuestas a dichos riesgos, permitiendo al auditor obtener evidencia suficiente y adecuada para reducir el riesgo de auditoría a un nivel bajo aceptable y así formar una opinión sobre los estados financieros. Durante todo este proceso, se requiere que el auditor ejerza su juicio profesional y mantenga un escepticismo profesional, reconociendo que pueden existir circunstancias que causen incorrecciones materiales. La NIA 315 (Revisada 2019) subraya que el proceso de identificación y valoración de riesgos es repetitivo y dinámico, adaptándose a la nueva información obtenida durante la auditoría.

La NIA 315 (Revisada 2019) profundiza en la identificación y valoración de los riesgos de incorrección material, definiéndolos como el riesgo de que los estados financieros contengan errores materiales antes de la realización de la auditoría.

Este riesgo se compone de dos elementos fundamentales:

Riesgo Inherente: Es la susceptibilidad de una afirmación a una incorrección que podría ser material, antes de considerar cualquier control. Este riesgo se ve influenciado por factores cualitativos o cuantitativos como la complejidad, la subjetividad, el cambio, la incertidumbre o la susceptibilidad a incorrecciones debido al sesgo de la dirección. El grado en que varía este riesgo se denomina "espectro de riesgo inherente".

Riesgo de Control: Es el riesgo de que una incorrección material no sea prevenida, o detectada y corregida oportunamente, por el sistema de control interno de la entidad. Se reconoce que siempre existirá cierto riesgo de control debido a las limitaciones inherentes del control interno, como el error humano o la posibilidad de elusión de controles por parte de la dirección.

Para llevar a cabo la identificación y valoración de estos riesgos, el auditor debe seguir un proceso estructurado que incluye:

a) Procedimientos de Valoración del Riesgo y Actividades Relacionadas: El auditor debe diseñar y aplicar estos procedimientos de manera imparcial para obtener evidencia que sirva de base para la identificación y valoración de riesgos. (Incluyen Indagaciones a la dirección; procedimientos analíticos que ayudan a identificar inconsistencias o tendencias inusuales que puedan indicar incorrecciones materiales; observación e inspección; entre otras).

b) Obtención de Conocimiento de la Entidad y su Entorno, el Marco de Información Financiera Aplicable y el Sistema de Control Interno: Este es un proceso continuo y dinámico de recopilación y análisis de información. Primero se debe comprender la estructura organizativa, propiedad y gobierno, y el modelo de negocio (incluyendo el uso de TI), luego entender los principios contables y las políticas de la entidad, así como las razones de cualquier cambio, también conocer cómo los factores de riesgo inherente (complejidad, subjetividad, cambio, incertidumbre, sesgo de la dirección) afectan la susceptibilidad de las afirmaciones a la incorrección y finalmente entender el sistema de control interno de una entidad.

c) Identificación y Valoración de los Riesgos de Incorrección Material:
Primero, en la identificación de los riesgos se identifican en dos niveles principales antes de considerar los controles, a nivel general de los estados financieros y en las afirmaciones.
Segundo, la valoración del riesgo inherente y el riesgo de control.

d) Evaluación de la Evidencia de Auditoría Obtenida: El auditor evalúa si la evidencia obtenida de los procedimientos de valoración de riesgos proporciona un fundamento adecuado para la identificación y valoración de estos, considerando tanto la evidencia corroborativa como la contradictoria.

e) Revisión de la Valoración del Riesgo: El proceso es dinámico; si se obtiene nueva información que difiera significativamente de la valoración inicial, el auditor debe revisarla.

f) Documentación: El auditor debe documentar los elementos clave de la discusión del equipo, el conocimiento de la entidad y sus controles, la evaluación del diseño e implementación de los controles, y la identificación y valoración de los riesgos de incorrección material (incluyendo los riesgos significativos y su justificación).

2. CONSIDERACIONES PARA EL CONOCIMENTO DE LAS TECNOLOGIAS DE LA INFORMACIÓN.

El sistema de control interno de una entidad se compone de cinco elementos interrelacionados:

1. Entorno de Control: Implica comprender la cultura de la entidad, el compromiso con la integridad y los valores éticos, la supervisión de la dirección y los responsables del gobierno, y la asignación de autoridad y responsabilidad. Se evalúa si proporciona un fundamento adecuado para los demás componentes.
2. Proceso de Valoración de Riesgos de la Entidad: Entender cómo la dirección identifica, evalúa y aborda los riesgos de negocio relevantes para la información financiera. Se considera si este proceso es adecuado para las circunstancias de la entidad.
3. Proceso de la Entidad para el Seguimiento del Sistema de Control Interno: Comprender las evaluaciones continuas y separadas para monitorear la eficacia de los controles y cómo se abordan las deficiencias. También se consideran las fuentes de información utilizadas para el seguimiento.

4. Sistema de Información y Comunicación: Entender cómo la información relevante para los estados financieros fluye, se inicia, registra, procesa, corrige y comunica, incluyendo el entorno de TI y cómo se utilizan las aplicaciones y la infraestructura de TI.
5. Actividades de Control: Identificar controles que aborden riesgos de incorrección material en las afirmaciones, como los controles sobre riesgos significativos, y aquellos que se planea probar por su eficacia operativa. Para cada control identificado, se evalúa su diseño y se determina si ha sido implementado.

En el contexto de las TI, el conocimiento del auditor de estos componentes es fundamental para identificar y valorar los riesgos de incorrección material.

La NIA 315 (Revisada 2019) establece que el auditor debe obtener un conocimiento de la entidad y de su entorno, incluido el sistema de control interno, para identificar y valorar los riesgos de incorrección material en los estados financieros, ya sea por fraude o error. Dentro de este análisis, las Tecnologías de la Información (TI) ocupan un rol central, ya que impactan directamente en la fiabilidad de la información financiera y en la eficacia de los controles internos.

A continuación, se detalla lo que el auditor debe conocer:

- Conocimiento del entorno de TI de la entidad:

El modelo de negocio de la entidad debe incluir hasta qué punto integra el uso de las TI. Esto ayuda al auditor a comprender los riesgos de negocio y cómo pueden afectar los estados financieros. Por ejemplo, una entidad que vende en línea procesa todas sus transacciones de venta en un entorno de TI, lo que conlleva riesgos de negocio diferentes a una tienda física.

El entorno de las TI abarca las aplicaciones de TI, la infraestructura que las soporta (red, sistemas operativos, bases de datos), y los procesos y personal involucrados en la gestión del acceso, cambios de programas y operaciones de TI.

- Identificación de aplicaciones de TI y otros aspectos del entorno de TI:

El auditor debe identificar las aplicaciones de TI y otros aspectos del entorno de TI que están sujetos a riesgos que surgen del uso de las TI. Estos riesgos se refieren a la susceptibilidad de los controles de procesamiento de información a un diseño u operación ineficaces, o a riesgos para la integridad de la información debido a controles ineficaces en los procesos de TI de la entidad.

La comprensión de los riesgos derivados del uso de TI y los controles generales de TI implementados es crucial, ya que esto puede influir en la decisión del auditor de probar la eficacia operativa de los controles, la valoración del riesgo de control, la estrategia para probar la información generada por la entidad, la valoración del riesgo inherente, y el diseño de procedimientos de auditoría posteriores.

- Controles de procesamiento de información y Controles generales de TI:

Para mitigar estos riesgos, la NIA 315 enfatiza la evaluación de los controles generales de TI, definidos como aquellos que respaldan el funcionamiento continuo adecuado del entorno de TI, asegurando la integridad, exactitud y validez de la información financiera. Incluyen:

- Seguridad de accesos en aplicaciones, bases de datos y sistemas operativos.
- Gestión de cambios en programas y configuraciones críticas.
- Monitoreo de operaciones de TI para prevenir interrupciones o pérdidas de datos.
- Seguridad de redes y protección frente a accesos externos.

Estos controles constituyen la base para la confiabilidad de los controles automatizados y permiten que el auditor evalúe si puede reducir el alcance de procedimientos sustantivos.

Escalabilidad del conocimiento de TI:

La naturaleza y el alcance del conocimiento de TI requerido por el auditor varían según el tamaño, la complejidad de la entidad y su entorno de TI.

En entidades menos complejas que utilizan software comercial sin acceso al código fuente, el conocimiento puede ser menos extenso, centrándose en cómo se gestionan los accesos y las actualizaciones del proveedor. Es poco probable que estas entidades necesiten o tengan controles generales de TI formalizados.

En contraste, entidades más grandes y complejas, que dependen en gran medida de TI con múltiples aplicaciones, requerirán un conocimiento más extenso de los procesos de TI y pueden necesitar la participación de miembros del equipo con habilidades especializadas en TI. En estos casos, es más probable que la entidad haya implementado controles generales de TI formalizados.

En resumen, el proceso de obtener conocimiento del sistema de control interno en un entorno de TI (incluida la IA y Blockchain) es dinámico y continuo. El auditor debe aplicar el juicio profesional para determinar la naturaleza y el alcance de los procedimientos a realizar, asegurando que se obtiene evidencia de auditoría suficiente y adecuada para identificar y valorar los riesgos de incorrección material.

En la versión revisada de la NIA 315 (2019) se incluyen dos anexos donde desarrollan cuestiones referidas a TI y control interno que debe tener en cuenta el auditor en un encargo.

Anexo 5: Consideraciones para conocer las Tecnologías de la Información (TI)

Este anexo tiene como objetivo proporcionar al auditor cuestiones adicionales a considerar para comprender el uso que hace la entidad de las TI en su sistema de control interno.

- Naturaleza de los elementos de control: El sistema de control interno de una entidad combina elementos manuales y automatizados (controles y otros recursos). La forma en que la entidad

utiliza las TI influye en cómo se procesa, almacena y comunica la información financiera, afectando el diseño e implementación del sistema de control interno.

- Beneficios de las TI para el control interno:
    - Aplicación consistente de normas predefinidas y realización de cálculos complejos.
    - Mejora en la oportunidad, disponibilidad y exactitud de la información.
    - Facilita el análisis adicional de la información.
    - Mejora la capacidad de seguimiento del rendimiento de las actividades.
    - Reduce el riesgo de elusión de controles.
    - Mejora la segregación de funciones eficaz mediante controles de seguridad.
- Fiabilidad de los controles: Los controles automatizados suelen ser más fiables que los manuales porque son menos propensos a ser omitidos, ignorados, anulados o a errores simples.
- Conocimiento del uso de TI en el sistema de información: El auditor debe recopilar información sobre la naturaleza y características de las aplicaciones de TI y la infraestructura de soporte utilizada para el procesamiento de información y los flujos de transacciones.
- Identificación de aplicaciones de TI sujetas a riesgos derivados del uso de TI: El auditor debe identificar en qué aplicaciones de TI confía la entidad para procesar la información financiera y mantener su integridad. Esto implica considerar los controles automatizados en los que la dirección confía, si hay acceso al código fuente, y la extensión de cambios en programas o configuraciones. Los informes generados por el sistema también pueden indicar aplicaciones sujetas a estos riesgos.
- Herramientas informáticas de usuario final: Aunque los resultados de estas herramientas pueden ser evidencia de auditoría, no suelen identificarse como aplicaciones de TI según la NIA 315. Se consideran controles de procesamiento de información, verificando la extracción de datos, fórmulas y macros.
- Otros aspectos del entorno de TI sujetos a riesgos: Cuando las aplicaciones de TI están sujetas a riesgos, otros aspectos de la infraestructura de TI como la base de datos, el sistema operativo y la red también suelen estarlo, ya que soportan e interactúan con dichas aplicaciones.

Anexo 6: Consideraciones para conocer los controles generales de TI

Este anexo proporciona información adicional que el auditor puede considerar al conocer los controles generales de TI. Se enfoca en la naturaleza de estos controles y ejemplos organizados por procesos de TI.

- Naturaleza de los Controles Generales de TI por capa del entorno de TI:
    - Aplicaciones: Se correlacionan con la funcionalidad de la aplicación y las rutas de acceso. Más controles son relevantes para aplicaciones integradas y complejas.
    - Base de datos: Abordan riesgos de actualizaciones no autorizadas de información financiera a través de acceso directo o ejecución de scripts.
    - Sistema operativo: Abordan riesgos relacionados con el acceso administrativo que podría anular otros controles (ej., comprometer credenciales, añadir usuarios no autorizados, instalar malware).
    - Red: Abordan riesgos relacionados con la segmentación de red, acceso remoto y autenticación. Relevante para aplicaciones web o transmisiones de datos con terceros.
- Ejemplos de Controles Generales de TI por Procesos de TI:
    - Proceso para gestionar el acceso:
        - Autenticación: Asegura que el usuario utiliza sus propias credenciales.
        - Autorización: Permite a los usuarios acceder solo a la información necesaria para sus tareas.
        - Aprovisionamiento: Controles para autorizar nuevos usuarios y modificaciones de privilegios.
        - Bajas: Controles para eliminar o modificar el acceso de usuarios al finalizar o transferirse.
        - Privilegios de acceso: Controles sobre el acceso administrativo o de usuarios con altos privilegios.
        - Revisiones de acceso de usuarios: Evaluaciones periódicas del acceso para autorización continua.
        - Controles de configuración de seguridad: Ajustes para restringir el acceso al entorno.
        - Acceso físico: Controles sobre el acceso físico al centro de datos y hardware.
    - Proceso para gestionar el programa u otros cambios en el entorno de las TI:
        - Proceso de gestión de cambios: Controles sobre el diseño, programación, prueba y migración de cambios al entorno de producción.
        - Segregación de funciones sobre migración de cambios: Separa el acceso para realizar y migrar cambios.

        - Desarrollo o adquisición o implementación de sistemas: Controles sobre la implementación inicial de aplicaciones o entornos de TI.
        - Conversión de datos: Controles sobre la conversión de datos durante el desarrollo, implementación o actualizaciones.
    - Proceso para gestionar las operaciones de TI:
        - Programación de trabajos: Controles sobre el acceso para programar e iniciar trabajos que afecten los informes financieros.
        - Seguimiento del trabajo: Controles para monitorear la ejecución exitosa de trabajos de informes financieros y corregir errores.
        - Copia de seguridad y recuperación: Controles para asegurar copias de seguridad regulares de datos financieros y disponibilidad para recuperación.
        - Detección de intrusión: Controles para monitorear vulnerabilidades o intrusiones en el entorno de TI.
- Tabla de Riesgos y Controles Generales de TI por tipo de aplicación: El anexo incluye una tabla detallada que muestra la aplicabilidad de los controles generales de TI (Gestión de Accesos, Gestión de Cambios, Operaciones de TI) a diferentes tipos de aplicaciones de TI según su complejidad (Software comercial no complejo, mediano/moderadamente complejo, grande/complejo (ERP)). Esta tabla ilustra cómo, por ejemplo, los controles de autenticación son aplicables en todos los niveles, mientras que la segregación de funciones para migración de cambios es más relevante en entornos de software no comercial o ERP complejos.

3. CONCLUCIONES

La NIA 315 (Revisada 2019) proporciona un marco integral y sistemático para que el auditor identifique y valore los riesgos de incorrección material en los estados financieros. Al enfatizar la importancia de comprender la entidad, su entorno y su sistema de control interno, la norma guía al auditor en la evaluación del riesgo inherente y de control de manera separada, lo que permite una respuesta de auditoría más precisa y eficaz. La distinción y el tratamiento específico de los "riesgos significativos" resaltan aquellas áreas que demandan una atención más profunda. Este proceso dinámico, sustentado en el juicio y escepticismo profesional, es fundamental para diseñar procedimientos de auditoría que conduzcan a la obtención de evidencia suficiente y adecuada, permitiendo al auditor expresar una opinión razonable sobre la fiabilidad de los estados financieros. La Norma Internacional de Auditoría (NIA) 315 (Revisada 2019) subraya que para obtener un conocimiento adecuado del sistema de control interno de una entidad, especialmente en un contexto cada vez más dependiente de la tecnología, el auditor debe profundizar en el entorno de las Tecnologías de la Información (TI), incluyendo el impacto de innovaciones como la Inteligencia Artificial (IA) y Blockchain. Este conocimiento es fundamental para identificar y valorar los riesgos de incorrección material en los estados financieros.

4. REFERENCIAS

International Auditing and Assurance Standards Board (IAASB). (2019, Diciembre). *Norma Internacional de Auditoría 315 (Revisada 2019): Identificación y valoración de los riesgos de incorrección material mediante el conocimiento*. Federación Internacional de Contadores (IFAC).

Escobar, D. S. (2025). Identificación de elementos para la elaboración de un marco conceptual no monetario de activos de información. Contabilidad y Auditoría, (61), 77-116.

Escobar, D. S. (2024). Evaluación de las prácticas de ciberseguridad en micro y pequeños estudios contables del AMBA. In JORNADA DE INVESTIGACIÓN. UNIVERSIDAD DEL SALVADOR FACULTAD CIENCIAS ECONÓMICAS Y EMPRESARIALES-USAL.

Escobar, D. S. (2024). Modelo capacitación y sensibilización en ciberseguridad para Contadores Públicos. In JORNADA DE INVESTIGACIÓN 2024. FACULTAD CIENCIAS ECONÓMICAS Y EMPRESARIALES-USAL.

Escobar, D. S. (2023). CIBERRESILIENCIA: UN NUEVO DESAFÍO EN LA FORMACIÓN DEL CONTADOR PÚBLICO. In XLIV Simposio Nacional de Profesores de Práctica Profesional. Universidad Nacional de Córdoba.

Escobar, D. S. (2023). Asegurando la Resiliencia Empresarial: Conceptos fundamentales a considerar en la auditoría de la continuidad del negocio. In XXXV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos. CGCE.

Escobar, D. S. (2023). Análisis de los cambios en los controles tecnológicos de la Comunicación A 7724 del BCRA en las entidades financieras. In XXXV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos. CGCE.

Escobar, D. S. (2023). EL IMPACTO DE LAS NUEVAS TECNOLOGÍAS DE INFORMACIÓN EN LA FORMACIÓN PROFESIONAL DEL CONTADOR. In XLIV Simposio Nacional de Profesores de Práctica Profesional. Universidad Nacional de Córdoba.

Escobar, D. S. (2023). La profesión contable ante los desafíos de la inteligencia artificial Chat GPT. In XXVI Congreso Nacional de Contabilidad. Colegio de Contadores del Paraguay.

Escobar, D. S. (2022). Requisitos mínimos de concientización para usuarios de Canales Electrónicos. Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, (2-3), 1-8.

Escobar, D. S. (2022). Identificación de estándares de seguridad de la información aplicables a los sistemas de información contable digitalizados. In XLIII Simposio Nacional de Profesores de Práctica Profesional. UNCUYO.

Escobar, D. S. (2022). Propuesta de un modelo contable que refleje el carácter de activo que la información corporativa representa para una entidad bancaria (Doctoral dissertation, Universidad de Buenos Aires (UBA)).

Escobar, D. S. (2022). El rol del Contador en la era digital. In VI Jornadas de Orientación Vocacional. UBA.

Escobar, D. S. (2022). Universo o dominio del discurso contable de los activos de información. In ECON 2022. UBA.

Escobar, D. S. (2022). Identificación de los riesgos de los registros contables alojados en servicios de computación en la nube. In XLIII Simposio Nacional de Profesores de Práctica Profesional. UNCUYO.

Kimura, E. B. S., & Escobar, D. S. (2021). Gestión de la ciberseguridad en sistemas contables digitalizados. In Ciclo" Universidades Iberoamericanas Dialogan". UBA.

Escobar, D. S. (2021). Mejores políticas para reducir los riesgos de alojar el sistema de información en la Nube. In ECON 2021. Facultad de Ciencias Económicas.

Escobar, D. S. (2018). Replanteo en el análisis de las contingencias, oportunidades y amenazas de los desvíos en los Estados Financieros Prospectivos. Gestión Joven, (18), 11.

5. BIBLIOGRAFIA

Las siguientes Normas Internacionales de Auditoría (NIA) son citadas dentro de la NIA 315 (Revisada 2019) y sus modificaciones de concordancia, sirviendo como referencias conceptuales y operativas para la aplicación de esta norma:

- NIA 200. (2009). *Objetivos globales del auditor independiente y realización de la auditoría de conformidad con las Normas Internacionales de Auditoría*.
- *NIA 315-ES. (2019) y Modificaciones de concordancia y en consecuencia a Otras Normas Internacionales que surgen de la NIA 315 (revisada 2019). Traducción al español.*