# *Article*

# *THE DIGITAL TRANSFORMATION OF AUDIT IN PUBLIC ADMINISTRATION: IMPACT OF NIA-ES 315 (REVISED)*

## 

**Laura Macau Pascual**

## *KEY WORDS:*

## Internal Audit, International Standards on Auditing, Digitisation, Public Sector, Cybersecurity, Advanced e-Government, Information Technology.

## *ABSTRACT:*

Digital transformation has had a significant impact on public administration auditing, driven by the adoption of advanced technologies and the revision of international standards. Digitalization has redefined the way in which administrative operations and processes are carried out, highlighting its relevance in internal audits of public entities. The implementation of the International Standard on Auditing adapted to the Spanish context, in particular NIA-ES 315 (Revised), has been a crucial turning point in addressing the challenges and opportunities arising from digitalization in the public sector. This standard provides a robust framework that empowers auditors to adapt effectively to an environment in constant technological transformation. Despite the benefits of digitization in improving transparency in public administrations, it is critical to address challenges such as the digital divide and ensuring data security and privacy.

***PALABRAS CLAVE:***

Auditoría interna, Normas internacionales de Auditoría, Digitalización, Sector público, Ciberseguridad, Administración Electrónica Avanzada, Tecnología de la información.

***RESUMEN:***

La transformación digital ha impactado significativamente en la auditoría de la administración pública, siendo impulsada por la adopción de tecnologías avanzadas y la revisión de estándares internacionales. La digitalización ha redefinido la forma en que se llevan a cabo las operaciones y procesos administrativos, destacando su relevancia en las auditorías internas de las entidades públicas. La implementación de la Norma Internacional de Auditoría adaptada al contexto español, en particular la NIA-ES 315 (Revisada), ha sido un punto de inflexión crucial para abordar los desafíos y oportunidades surgidos de la digitalización en el sector público. Esta normativa proporciona un marco sólido que capacita a los auditores para adaptarse eficazmente a un entorno en constante transformación tecnológica. A pesar de los beneficios de la digitalización en la mejora de la transparencia en las administraciones públicas, es fundamental abordar los desafíos como la brecha digital y garantizar la seguridad y privacidad de los datos.

***MOTS CLÉS :***

Audit interne, Normes internationales d'audit, numérisation, secteur public, cybersécurité, administration en ligne avancée, technologies de l'information.

***RÉSUMÉ :***

La transformation numérique a eu un impact significatif sur l'audit de l'administration publique, sous l'effet de l'adoption de technologies avancées et de la révision des normes internationales. La numérisation a redéfini la manière dont les opérations et les processus administratifs sont menés à bien, soulignant sa pertinence pour les audits internes des entités publiques. La mise en œuvre de la norme internationale d'audit adaptée au contexte espagnol, en particulier la norme NIA-ES 315 (révisée), a constitué un tournant décisif pour relever les défis et saisir les opportunités découlant de la numérisation dans le secteur public. Cette norme fournit un cadre solide qui permet aux auditeurs de s'adapter efficacement à un environnement technologique en constante évolution. Malgré les avantages de la numérisation pour améliorer la transparence dans les administrations publiques, il est essentiel de relever des défis tels que la fracture numérique et la garantie de la sécurité et de la confidentialité des données.

## *1. INTRODUCTION*

In the era of digital transformation, auditing in public administration has undergone a significant evolution, driven by the adoption of advanced technologies and the revision of international standards. Digitalisation has burst into the public sector as a catalyst for change, profoundly transforming the way administrative operations and processes are carried out. This change has been particularly relevant in the field of internal audits in public administrations, where the adoption of digital technologies has proven to be crucial to improve the efficiency, transparency and effectiveness of audit processes.

NIA-ES 315 (Revised), hereafter referred to as NIA-ES 315R, represents a fundamental standard-setting framework that guides the auditor's work in obtaining a comprehensive understanding of the audited entity's environment, including an assessment of the internal controls relevant to the audit process. As will be explained in subsequent sections, this standard provides updated guidance for risk assessment and audit planning, specifically tailored to the particularities and complexities inherent in public sector entities.

The purpose of this article is to take a closer look at the technological transformation of internal auditing in the public sector, focusing on the application of NIA-ES 315R as a key framework. It will discuss how digital technologies are being used to improve the efficiency and effectiveness of internal audit, as well as the specific challenges and opportunities facing auditors in advanced e-government environments.

***2. THE DIGITAL EVOLUTION OF LOCAL AUTHORITIES***

The digital evolution in public administration has been a process of progressive and significant transformation, driven by the imperative need to improve operational efficiency, management transparency and the quality of services offered to citizens. In this context, the adoption and implementation of ERP systems has played a key role in the modernisation of administrative practices, enabling more effective management and decision-making based on reliable and timely data.

Historically, public administration has faced challenges inherent in the availability of reliable information, the optimisation of processes and the need to share data between different areas of the organisation. The introduction of ERP systems has been key to overcoming these barriers by enabling the integration of different areas into a centralised, comprehensive and up-to-date database. This approach has facilitated the control and auditing of processes, providing management with a holistic view of the organisation and improving audit planning[[1]](#footnote-1).

As mentioned above, the context in public administrations has changed completely. The beginning of this revolution can be traced back to laws 39/2015[[2]](#footnote-2) and 40/2015[[3]](#footnote-3) from that moment onwards, all public administration was progressively computerised, to the point that in recent years the administration has been managed almost exclusively by means of computerised systems. These laws have given a significant boost to e-administration, transforming the way in which administrative procedures are carried out, public resources are managed and interaction with citizens takes place.

Today we have various electronic administrative procedures by default, such as: electronic files, electronic invoices, electronic procurement... In short, everything is done with complex computer applications, massive databases, integrated systems and, therefore, with zero paper. Moreover, all the controls to be carried out are either automated or based on information systems. This has a very direct implication for the work of auditors, understanding that they are both external auditors and auditors themselves.

It is important to understand this process of public digitisation and for this we can highlight several main stages. We start from a traditional administration, basically analogue, in which computers were introduced and computers were an auxiliary element, which were used to carry out the processes, which were basically analogue.

In this way, the analogue processes were progressively computerised in the electronic administration stage, which we call computerization. In recent years, the computerisation of processes has taken a qualitative leap, thus entering the stage of advanced electronic administration, hereinafter AEA, in which administrations have undergone the process of digital transformation.

AEA is characterised by three basic features, which are what determine whether this transformation process has taken place. First, there is the fact that there has been a re-engineering of processes, leaving behind the analogue processes supported by computers. The second characteristic would be that, with the help of increasingly complex computer applications, public management processes have been redesigned with the help of these complex information systems. Thus, today's process systems allow us to work in an optimised and efficient way. The last characteristic is that complex information systems are massively interconnected. If all three characteristics are present, we can say that the digital transformation has taken place and that we are therefore dealing with an advanced eGovernment.

***2.1. Challenges and considerations of digitisation***

The digital transformation in the field of public administration has generated a substantial change in the management of government functions. This process, driven by technological advances and the growing demand for efficient services, has focused attention on auditing as a guarantor of integrity and transparency in the use of public resources.

In this context, the implementation of the International Standard on Auditing (ISA) adapted to the Spanish context, particularly NIAS-ES 315 (Revised), has been a significant turning point. This standard has been designed to address the challenges and opportunities arising from digitalisation in public administration, providing a robust framework that empowers auditors to adapt effectively to an environment characterised by rapid technological transformation.

Despite the benefits of digitisation to improve transparency in public administrations, there are important challenges and considerations to take into account. These include the digital divide, which may exclude certain groups of the population from accessing information online, as well as concerns about data privacy and security. It is crucial to address these challenges proactively and ensure that digitisation is implemented in an inclusive and secure manner for all citizens.

*2.1.1. Transparency of public administrations*

Transparency in public administrations is a fundamental principle to promote citizen trust and ensure accountability. Digitalisation has emerged as a tool to improve transparency in the public sector by facilitating access to information and promoting citizen participation.

Digitisation has made public information more accessible, facilitating its dissemination through online platforms and government portals. Citizens can now easily access relevant documents, reports, data and statistics on government management. This active transparency fosters greater citizen participation by empowering individuals with information to make informed decisions and exercise effective control over the actions of their representatives.

In addition, the digitisation of administrative and financial processes has improved transparency in the management of public resources. Integrated financial management systems, e-procurement platforms and budget tracking tools provide a detailed overview of how public funds are allocated and used. This transparency in financial management helps prevent corruption, optimise the use of resources and improve efficiency in the implementation of government policies and programmes.

*2.1.2. Cybersecurity*

When we talk about digital transformation, we must inevitably talk about cybersecurity. According to Regulation (EU) 2019/881, cybersecurity refers to all activities necessary for the protection of networks and information systems, the users of such systems and other persons affected by cyber threats.

Cybersecurity is one of the essential aspects that today requires a large amount of resources, both technological and human, in-house and from third parties. Budget chapters two and six require programmed and coherent efforts for a working environment prepared to deal with these risks. The necessary compliance with the National Security Scheme[[4]](#footnote-4) (NSS) and data protection may be an opportunity to promote proactive policies in this regard.

Article 33 of RD 424/2017[[5]](#footnote-5) requires the auditors to "verify the security and reliability of the IT systems that support the economic-financial and accounting information". It is also required by NIA-ES-SP.

NIA-ES 315R[[6]](#footnote-6) requires the auditor to identify appropriate cybersecurity governance. Governance is the process of establishing and maintaining a framework for making all security measures work. The confidentiality, integrity, availability, traceability and authenticity of data must be ensured. In other words, cybersecurity seeks to protect the information assets processed, stored and transported by interconnected networks and information systems. Controls to protect these assets and ensure compliance with the above characteristics are part of general information technology controls (GITC).

In addition, NIA-ES 315R in paragraph 26 states that the auditor should obtain sufficient knowledge of how the audited entity uses information systems, the design and operation of automated controls and their impact on the financial statements.

Cybersecurity has become a crucial concern for the public and private sector due to the steady increase in cyber-attacks. Public auditors should consider these risks when performing audits of annual accounts in accordance with NIA-ES 315 (Revised).

Technological integration in public entities, accelerated by teleworking during the pandemic, has generated an advanced digital environment characterised by all-digital management, extensive use of interconnected applications, automated internal controls, cloud computing, large databases and emerging technologies such as blockchain and artificial intelligence.

Despite the opportunities, increased connectivity and reliance on the internet increase the risk of cyber-attacks, which can cause loss of information, manipulation of data and damage to physical assets, with significant impact on annual accounts. Auditors should therefore pay particular attention to these growing risks.

***3. INTERNATIONAL STANDARDS ON AUDITING***

For context, it should be mentioned that NIAs are the International Standards on Auditing issued by the International Auditing and Assurance Standards Board (IAASB) through the International Federation of Accountants (IFAC)[[7]](#footnote-7). These standards have been created with the objective of uniting and standardising audit methodologies, providing unified guidelines for performing audits with assurance. They consist of five fundamental components: preamble, purpose, terminology, guidelines and additional explanatory material and are considered fundamental to the integrity and transparency of the global financial system.

Therefore, NIAs are essential to ensure a certain quality, credibility and confidence in financial reports issued in a globalised environment.

In Spain, the Instituto of Contabilidad y Auditoría de Cuentas (ICAC) adopts and adjusts the NIAs to adapt them to local reality and regulations, thus facilitating their application in the national context.

***3.1. Evolution of NIA-ES 315 to NIA-ES 315 (Revised)***

The subject of this article is NIA-ES 315 R, which is a 2019 update of NIA-ES 315. This standard, NIA-ES 315, was adopted in 2003 and has remained in force and unchanged in content until the adoption of NIA-ES 315R. NIA-ES 315 provided for the identification and assessment of the risks of material misstatement through knowledge of the entity and its environment, essentially like the current revised NIA. Thus, NIA 315 was intended to be used by the auditor as audit evidence to support such assessments. The analytical processes described in the standard are able to identify the existence of transactions and amounts that are materially misstated, which helps to understand whether certain processes are having complications for the audit by identifying the risks of material misstatement[[8]](#footnote-8). In addition to identifying, it also aims to assess these risks, classify them as fraud or error, and respond to them.

In this way, the context in which the standard was created must be considered. At the time, the audited entities, both private and public, were in a fundamentally similar management environment. This fact has been changing over the years, until today, where audited environments of advanced e-government can be observed, in which data are digitally interconnected.

Therefore, it is obvious that the methodology used to carry out audits must change, and at the same time, the regulations must be adapted to the new technological reality. This need to conduct audits in digital environments was the impetus for a review of the standards in force at the time.

It is in this context that NIA-ES 315 (Revised) was published in the resolution of 14 October 2021 of the Spanish Accounting and Auditing Institute. From this same resolution, two other Technical Auditing Standards emerged as a result of the adaptation of the NIAs for their application in Spain: NIA-ES 250 (Revised) and NIA-ES 610 (Revised). It should be remembered that these standards will be mandatory for audits of annual accounts or other financial statements or accounting documents corresponding to financial years beginning on or after 1 January 2022, as well as for those commissioned on or after 1 January 2023, regardless of the financial years to which their financial statements refer[[9]](#footnote-9).

Thus, NIA-ES 315R builds on NIA-ES 315 and therefore also aims to describe the responsibility of auditors to identify and properly assess the risks of material misstatement in financial statements.

Although the new standard builds on the previous standard, requirements have been incorporated to require a more robust identification and assessment of risk in order to propose the most appropriate responses to these risks[[10]](#footnote-10).

In addition, NIA-ES 315R also improves the aspect of clarity and explanatory consistency, as well as considerably better specifying the procedures and applications to be followed.

***4. NIA-ES 315 (REVISED)***

As mentioned above, NIA-ES 315R is intended, on the one hand, to bring the standards into line with the digital reality and, on the other hand, to improve the structure of the standards to make it easier for auditors to apply them in practice. It should therefore be remembered that the auditor's role is to use the methodology presented in the standards to identify and assess risks of material misstatement and to respond to and address those risks.

In this way, the standard in question is based on the applicable financial reporting framework and the audited entity's internal control system. In addition, this standard represents a very significant advance over the previous version, as it facilitates audit work in advanced e-government environments. It also helps to manage the effect of auditees' use of IT on all aspects of the audit methodology by introducing guidance that recognises the changing IT environment including the use of emerging technologies. It also highlights the growing importance of cybersecurity, which will be developed in subsequent sections.

***4.1. Changes implemented in NIA-ES 315R***

As can be seen in the previous section, NIA 315R has improved on the previous standard in several respects.

One of the most important changes is the specific incorporation of elements to identify control activities. In this regard, the previous standard simply required the identification of "controls relevant to the audit", which were scattered in different standards and led to different interpretations and, therefore, inconsistent practice. However, the IAASB grouped all controls relevant to the identification of risks in the same standard[[11]](#footnote-11). The existing controls are as follows and are found in paragraphs A147-A157 of the standard:

1. Controls that address a risk considered significant.
2. Controls over accounting entries.
3. Controls that determine the nature, timing and substantive testing for the purpose of determining operational effectiveness.
4. Controls over the auditor's professional judgement.

The latter control introduces a new concept called the inherent risk spectrum. This concept means that the auditor is given the freedom to apply his own professional judgement when he considers that there is a high likelihood of a material misstatement. This range of possibilities is then referred to as the inherent risk spectrum.

To differentiate the above concept from significant risk, the definition of significant risk has been redefined. The previous standard defined significant risk as "in the auditor's judgement, requires special consideration in the audit". NIA-ES 315R specifies that it is an identifiable risk when the risk is near the upper end of the inherent risk spectrum, considering the combination of the likelihood of its existence and the magnitude of the potential risk[[12]](#footnote-12).

The new requirements are therefore intended to assist auditors to identify and assess the risks of material misstatement more consistently.

Therefore, it can be stated that the changes made to the standard have managed to ease the complexity of the structure of NIA 315, thus achieving a clearer and more understandable text. However, it should be borne in mind that in order to better organise the subject matter, various sections have been added which have made this standard considerably longer than its predecessor. Even so, it is considered an achievement, as the new reorganised structure with annexes makes the practical application of the regulation much easier. In addition, new sections have been added, such as "key concepts", among others, which make it easier to distinguish and use the different existing NIAs.

On the other hand, NIA-ES-315R has been updated with regard to the aspects related to an internal control system with the intention of unifying criteria and adapting them to the provisions of COSO 2013. This is one of the elements that the revised version highlights, but which we already had in the previous version. The five fundamental components to which it refers are as follows:

1. The control environment: Emphasises the importance of understanding and assessing the entity's governance of IT, including the complexity or maturity of the platform. It is also important to see whether investment has been made in an adequate IT environment and whether the necessary upgrades and staffing have been carried out.
2. The entity's risk assessment process
3. The entity's process for monitoring the internal control system.
4. The information and communication system: We must know the ICS, how it is used and identify the risks derived from this use of IT. It is also essential to know the IT resources and environment, which are made up of:
   * IT applications
   * IT infrastructure: which supports IT and comprises network hardware and software, operating systems and databases.
   * IT processes
   * IT staff
5. Control activities. NIA-ES 315R in Article 26 requires identifying:
   * Information processing controls (IPCs) that respond to RIM in assertions.
   * IT applications subject to risk
   * aspects of the IT environment that are subject to risk
   * Risks arising from the use of IT.
   * General IT controls (GITC) that respond to risks.

As mentioned above, NIA-ES 315R explicitly states in paragraph 26 the importance for auditors to fully understand the control activities component of the internal control system by applying risk assessment procedures, thereby identifying the entity's General Information Technology Controls (GITC) that directly address risks related to the use of information technology (IT).

It is important to note that NIA-ES 315R is a lengthy and complex standard and the Technical Committee of External Audit Bodies (OCEX) has developed practical guides for the audit of OCEX (GPF-OCEX). These guides are basically based on NIA-ES 315R, are fully descriptive and are intended to help OCEX auditors to understand the main changes introduced in this new standard. The intention behind the creation of these guides is to further facilitate the transformation from theory to practice and thereby assist and streamline the work of auditors[[13]](#footnote-13).

The guides based on this legislation and relevant to the topic of study are as follows:

* + GPF-OCEX 1315 Identifying and assessing the risks of material misstatement through an understanding of the entity and its environment.
  + GPF-OCEX 1316 The required knowledge of the entity's internal control.
  + GPF-OCEX 1317 Guidance on Identifying and Assessing the Risks of Material Misstatement.
  + GPF-OCEX 5330 Review of General IT Controls in an e-Government Environment.
  + GPF-OCEX 5340 Application controls: what they are and how to review them.

From this guide, we can highlight the recommendation it makes on the possibility of incorporating new members with specialised IT qualifications into the teams. This would create teams with different areas of expertise, bringing together financial auditors with information systems and cybersecurity auditors. Thus, NIA-ES 315R establishes the importance of auditors and auditors adapting to the AEA, but also makes it clear that it is not mandatory for them to be specialists in everything and that therefore the possibility is given to recruit specialists in these matters.

***4.2. Application of NIA-ES 315R: Automated Risk Assessment Tools***

The updated NIA-ES 315R recognises and evidences the need to regulate the increasing use of automated tools and techniques applied in audit procedures. Therefore, the standard establishes in several sections’ requirements for the use of these automated tools and techniques. Thus, when an auditor performs an audit of an entity, he/she must apply the procedures described in the standards to assess the risks and additionally the use of these automated tools is foreseen to achieve the objective of risk identification and assessment. For the purposes of an audit, then, these automated tools and techniques are IT-driven processes that may involve the automation of many procedures, as well as the use of artificial intelligence for the inspection of assets[[14]](#footnote-14). In this sense, the auditor has the possibility to use these digitised processes to gain download or direct access to a database of an information system. They can also review transactions or keep track of journal entries or digital records.

The most commonly used automated tools are the following[[15]](#footnote-15):

* Data analysis: to evaluate complete data sets, identifying and analysing patterns and trends, unusual elements and deviations.
* Robotic Process Automation (RPA): This is performed by software that quickly and accurately performs repetitive mechanical activities for the processing of structured data.
* Artificial intelligence techniques: This uses technology that is able to recognise certain patterns in massive amounts of data, including unstructured data such as emails, social media content, contracts, invoices, images and audio files from telephone meetings.

Auditors can use artificial intelligence to gather information from various sources to assist the auditor in identifying risks of material misstatement. Applying such procedures and tools, in accordance with NIA-ES 315R, enables the auditor to obtain detailed and advanced knowledge about the audited business or activity in a much faster and more efficient manner.

***4.3. Adapting NIA-ES 315R to public sector entities***

The digital evolution in the field of audit and assurance has been a topic of increasing relevance due to the impact of advanced technologies, such as artificial intelligence (AI), on the way audits are conducted. The International Auditing and Assurance Standards Board (IAASB) has recognised the importance of adapting to these technological developments to ensure the quality and effectiveness of audits in an increasingly digitalised business environment. In this context, the IAASB has been assessing how international standards on auditing (NIAs/ISAs) can foster innovation in the audit services market.

As we can see, the environments in public administrations have changed and the current environment is one characterised by AEA, so the public auditor must understand the complexity involved and adapt accordingly.

Fortunately, the new NIA-ES 315R is designed for auditing in today's technological environments, with digital administration and the use of integrated management software applications (ERP). This is why this law devotes a large part of its content to the identification of risks, both digital and non-digital, so that it can be used in any environment and be adaptable in any current audit situation. Thus, there are already many professionals who consider that this regulation should be applied in public entities, given that there is no law exclusively for this environment, but due to its characteristics, this law is an appropriate option for solving the problems faced by public administration today.

The rationale behind NIA-ES 315R is that it is a methodology to be followed, which makes it a perfect candidate because of its adaptability to public sector entities. Auditors or auditors should apply the methodology presented in their particular working environment with the digital resources available to them. For this reason, NIA-ES 315R requires auditors to obtain a minimum knowledge of the technology to be used and above all to have studied the audited entity.

Therefore, Annex 1 of NIA-ES 315R defines the risks arising from the use of IT as the exposure of information processing controls to ineffective design or operation. On the other hand, Royal Decree 424/2017 of 28 April, which regulates the legal regime of internal control in Local Public Sector entities, hereinafter RCIL, already incorporated in its regulation the definition of risk, placing it in the scope of public sector auditing. This regulation also highlights the importance and essential need for auditors to identify risks or potential risks within the entity. As has been emphasised throughout the presentation, a risk analysis is essential for a proper audit. This study is carried out by the local Financial Controller, who is in charge of internal control, given that article 6.1 of the RCIL gives him the power to review computerised management systems.

Although this law introduces the concept of risk, it has the disadvantage that it does not provide a methodology to be followed, so article 29.4 refers the application to the financial control and public audit standards in force. This is how the RCIL is related and linked to the NIAS. Firstly, it was related to NIA-ES-SP 1315, given that it is the previous standard that identifies and assesses risks, but given its age and outdatedness, it is not very applicable to current audits. For this reason, the standard currently used is NIA-ES 315R which identifies and assesses risks more clearly and from a more contemporary point of view, considering the effects of technology on the auditor's work.

Finally, it is worth mentioning that, although there are regulations that establish a methodology to be followed, in practice, the risk analyses carried out by most local auditors are based on a very subjective analysis, as it will always depend to a large extent on the judgement and choice of the auditor himself. This will be based on his or her previous experience, knowledge of the environment, the budget available to him or her, among others. As Mari Carmen Aparisi, a senior financial controller,[[16]](#footnote-16) explains, this can involve a double risk: on the one hand, an objective risk analysis cannot be carried out for several reasons, including the lack of available resources, both materials, human and technical, and on the other hand, the financial controller himself is involved in the budget management processes and in the management and keeping of the accounts. For all these reasons, there is no real separation of powers, which limits the objectivity of the procedure, as only municipalities classified as having a large population are eligible.

***5. CONCLUSIONS***

Digital transformation has revolutionised auditing in public administration, driven by the adoption of advanced technologies and the updating of international standards such as NIA-ES 315R. This framework has been instrumental in guiding auditors in assessing risks, understanding the audited entities' environment and planning audits tailored to the particularities of public entities.

The digital evolution in local entities has been a progressive and significant process, driven by the need to improve operational efficiency, transparency in management and the quality of services offered to citizens. The implementation of ERP systems has been key to this modernisation, enabling more effective management and decision-making based on reliable and timely data.

Digitalisation has generated a substantial change in the management of government functions, focusing attention on auditing as a guarantor of integrity and transparency in the use of public resources. The adaptation of the International Standard on Auditing to the Spanish context, especially NIA-ES 315R, has been a significant turning point to face the challenges and opportunities arising from digitalisation in public administration.

Despite the benefits of digitisation to improve transparency in public administrations, there are important challenges such as the digital divide and concerns about data privacy and security. It is crucial to address these challenges proactively and ensure that digitalisation is implemented in an inclusive and secure manner for all citizens.

In summary, digital transformation has redefined auditing in public administration, highlighting the importance of adapting to technological advances to ensure efficiency and transparency in the management of public resources in an increasingly digitised environment.

***6. REFERENCES***

ASOCEX - Revista de los órganos autonómicos de control Externo Nº80

Auditool - Principales cambios en la NIA 315 (Revisada)

Colegio de Economistas de Madrid - NIA-ES 315 Revisada: <https://www.cemad.es/wp-content/uploads/2023/02/NIA-315-1.pdf>

Ecovis Grosclaude & Partners - Novedades NIA-ES 315 (Revisada), Identificación y valoración del riesgo de incorrección material (Enero 2023): <https://www.grosclaude.es/wp-content/uploads/2023/01/NIA-ES-315-v001_09.01.23.pdf>

IAASB Main Agenda (March 2024) - Technology Position - Introduction to Development: <https://www.iaasb.org/_flysystem/azure-private/2024-03/20240318%20-%20Agenda%20Item%204%20-%20Technology%20Position_Introduction%20to%20Development_Final_0.pdf>

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: <https://www.ifac.org/_flysystem/azure-private/publications/files/Technology-FAQ_Automated-Tools-and-Techniques_ISA-315-Revised-2019_ES_Secure_0.pdf>

IAASB, Introducción a NIA 315 (Revisada) Identificación y valoración del riesgo de incorrección material, 2019: <https://www.ifac.org/_flysystem/azure-private/publications/files/IAASB_Introduction-to-ISA-315_Revised-2019_ES_Secure_0.pdf>

IAASB, Preguntas frecuentes sobre tecnología y la utilización de herramientas técnicas automatizadas para la realización de procedimientos de valoración del riesgo, de conformidad con la NIA 315 (Revisada 2019), Noviembre 2020: <https://www.ifac.org/_flysystem/azure-private/publications/files/Technology-FAQ_Automated-Tools-and-Techniques_ISA-315-Revised-2019_ES_Secure_0.pdf>

IFAC - El proceso de identificación y evaluación de riesgos consejos para aplicar la NIA 315 (Revisada) <https://ifacweb.blob.core.windows.net/publicfiles/2023-07/IFAC-ISA-315-Material-Misstatement-Implementation-Tool-Auditors%20%28español%29-locked.pdf>

Jimémez Rus, Pilar - Una nueva Auditoría Pública (Setiembre, 2020)

Joan Ballesteros - Sinfopac - Cambios en la norma internacional de auditoría 315 - <https://sinfopac.com/es/noticias/actualidad/nia-315-revisada-principales-cambios>¡

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas: <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565>

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público: <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566>

Minguillón Roy, Antonio - Auditoría de cuentas anuales y Ciberseguridad: la nueva NIA-ES 315(Revisada) y el auditor público, Serie Opiniones FIASEP, Nº 13/2022 de abril 2022.: <https://fundacionfiasep.org/2022/04/11/opinion-13-auditoria-de-cuentas-anuales-y-ciberseguridad-la-nueva-nia-es-315-revisada-y-el-auditor-publico/>

Minguillón Roy, Antonio - La NIA-ES 315 (revisada) Identificación y valoración del riesgo de incorrección material y su impacto inmediato en la actividad del auditor público en un entorno de administración electrónica avanzada: <https://fundacionfiasep.org/wp-content/uploads/2022/06/Opinion-no14.-Principales-novedades-NIA-ES-315Revisada-v25-5-2022.pdf>

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.: <https://fundacionfiasep.org/wp-content/uploads/2022/06/Opinion-no14.-Principales-novedades-NIA-ES-315Revisada-v25-5-2022.pdf>

Real Decreto 424/2017, de 28 de abril, por el que se regula el régimen jurídico del control interno en las entidades del Sector Público Local: <https://www.boe.es/buscar/act.php?id=BOE-A-2017-5192>

Sindicatura de Comptes de la Comunitat Valenciana - Manual de fiscalización de la Sindicatura de Comptes 2023: [www.sindicom.gva.es/manual-de-fiscalizacion-2023](http://www.sindicom.gva.es/manual-de-fiscalizacion-2023)

The Consideration of Cyber Security Risks in an Audit of a Financial Report, Australian Auditing and Assurance Standards Board, Boletín de mayo de 2021

1. Ángelo Benvenuto - Implementation of ERP systems, their impact on business management and integration with other ICTs. [↑](#footnote-ref-1)
2. Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations: <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565> [↑](#footnote-ref-2)
3. Law 40/2015, of 1 October, on the Legal Regime of the Public Sector: <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566> [↑](#footnote-ref-3)
4. Royal Decree 311/2022 of 3 May, which regulates the National Security Scheme: <https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191>) [↑](#footnote-ref-4)
5. Royal Decree 424/2017, of 28 April, which regulates the legal regime of internal control in the entities of the Local Public Sector. [↑](#footnote-ref-5)
6. NIA-ES 315 (revised). Identifying and Assessing the Risk of Material Misstatement [↑](#footnote-ref-6)
7. Guillermo Westreicher, May 23, 2021, International Standards on Auditing (NIAs). [↑](#footnote-ref-7)
8. Ana Belén Delgado - What does NIA 315 establish? [↑](#footnote-ref-8)
9. Ecovis Grosclaude & Partners - News NIA-ES 315 (Revised) - January de 2023 [↑](#footnote-ref-9)
10. IAASB Fact Sheet Introduction to NIA 315 (Revised) Identifying and Assessing the Risks of Material Misstatement [↑](#footnote-ref-10)
11. Internacional Federation of Accountants - The process of risk identification and assessment [↑](#footnote-ref-11)
12. Article 12.l of NIA-ES 315R [↑](#footnote-ref-12)
13. Minguillón Roy, Antonio - Serie opiniones FIASEP Nº14/2022 [↑](#footnote-ref-13)
14. NIA-ES 315R, paragraph 35 [↑](#footnote-ref-14)
15. IAASB, Frequently Asked Questions on Technology - November 2020 [↑](#footnote-ref-15)
16. Aparisi, Mari Carmen - Practical issues for the implementation of e-audit in local governance [↑](#footnote-ref-16)