C. Mallorca 260
08008 Barcelona
Tel. 932 155 989
www.auren.com

auren

A PROP TEU PER ARRIBAR LLUNY

14º JORNADA DE AUDITORIA DEL SECTOR PUBLICO

LOS RETOS TECNOLÓGICOS Y LA GESTIÓN DE RIESGOS

27 ABRIL 2023

Albert Lladó
CISA, CISM, CGEIT, CRISC, LA27K, LA22301,
Ingeniero, MUDIGIT, MBA
Socio GRC AUREN
Fundador, Past Presidente, Vocal Relaciones Institucionales ISACA_BCN

Albert.llado@isacabcn.org
Albert.llado@auren.es

- Introducción
- Conceptos y requisitos: ENS
- Otros Marcos de referencia: ISO27k
- RGPD
- Relación RGPD y ENS
- Conclusiones

- **Introducción**
- Conceptos y requisitos: ENS
- Otros Marcos de referencia: ISO27k
- RGPD
- Relación RGPD y ENS
- Conclusiones

Introducción

NORMA INTERNACIONAL DE AUDITORÍA 315

IDENTIFICACIÓN Y VALORACIÓN DE LOS RIESGOS DE INCORRECCIÓN MATERIAL MEDIANTE EL CONOCIMIENTO DE LA ENTIDAD Y DE SU ENTORNO

(NIA-ES 315 adaptada para su aplicación al Sector Público Español, NIA-ES-SP 1315, aprobada mediante Resolución de la Intervención General de la Administración del Estado, de 25 de octubre de 2019)

NORMA INTERNACIONAL DE AUDITORÍA 315 (REVISADA)

IDENTIFICACIÓN Y VALORACIÓN DEL RIESGO DE INCORRECCIÓN MATERIAL

NIA-ES 315 (REVISADA)

(adaptada para su aplicación en España mediante Resolución del Instituto de Contabilidad y Auditoría de Cuentas, de 14 de octubre de 2021)

NIA ES-SP 1315

Alcance de esta NIA-ES-SP

1. Esta Norma Internacional de Auditoría adaptada al Sector Público Español (NIA-ES-SP) trata de la responsabilidad que tiene el auditor de identificar y valorar los riesgos de incorrección material en los estados financieros, mediante el conocimiento de la entidad y de su entorno, incluido el control interno de la entidad.

.....

(c) Control interno: el proceso diseñado, implementado y mantenido por los responsables del gobierno de la entidad, la dirección y otro personal, con la finalidad de proporcionar una seguridad razonable sobre la consecución de los objetivos de la entidad relativos a la fiabilidad de la información financiera, la eficacia y eficiencia de las operaciones, así como sobre el cumplimiento de las disposiciones legales y reglamentarias aplicables. El término "controles" se refiere a cualquier aspecto relativo a uno o más componentes del control interno.

.....

El conocimiento requerido de la entidad y su entorno, incluido su control interno

NIA-ES 315 R

Definiciones

(d) *Controles generales de las tecnologías de la información (TI)*: 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 integridad, exactitud y validez de la información) en el sistema de información de la entidad. Véase también la definición de *entorno de TI*.

(e) *Controles del procesamiento de la información*: 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 integridad, exactitud y validez de las transacciones y otra información). (Ref: Apartado A6)

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

(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.

NIA-ES 315 R

Definiciones

.....

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

NIA ES-SP 1315

El proceso de valoración del riesgo por la entidad

.....

18. El auditor obtendrá conocimiento del sistema de información, incluidos los procesos de negocio relacionados, relevante para la información financiera, incluidas las siguientes áreas:

(a) los tipos de transacciones en las operaciones de la entidad que son significativos para los estados financieros;

(b) los procedimientos, relativos tanto a las tecnologías de la información (TI) como a los sistemas manuales, mediante los que dichas transacciones se inician, se registran, se procesan, se corrigen en caso necesario, se trasladan al libro mayor y se incluyen en los estados financieros;

(c) los registros contables relacionados, la información que sirve de soporte y las cuentas específicas de los estados financieros que son utilizados para iniciar, registrar y procesar transacciones e informar sobre ellas; esto incluye la corrección de información incorrecta y el modo en que la información se traslada al libro mayor; los registros pueden ser tanto manuales como electrónicos;

(d) el modo en que el sistema de información captura los hechos y condiciones, distintos de las transacciones, significativos para los estados financieros;

(e) el proceso de información financiera utilizado para la preparación de los estados financieros de la entidad, incluidas las estimaciones contables y la información a revelar significativas; y

(f) los controles sobre los asientos en el libro diario, incluidos aquellos asientos que no son estándar y que se utilizan para registrar transacciones o ajustes no recurrentes o inusuales. (Ref.: Apartados A81-A85)

NIA ES-SP 1315

Objetivos y estrategias, así como riesgos de negocio relacionados (Ref.: Apartado 11(d))

.....

- Requerimientos normativos (un riesgo de negocio potencial relacionado puede ser, por ejemplo, una mayor vulnerabilidad desde un punto de vista jurídico).

.....

- La utilización de TI (un riesgo de negocio potencial relacionado puede ser, por ejemplo, que los sistemas y procesos sean incompatibles).

División del control interno en componentes

NIA-ES 315 R

.....

19. El auditor aplicará procedimientos de valoración del riesgo para obtener conocimiento de:

(a) los siguientes aspectos de la entidad y su entorno:

(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; (Ref: Apartados A56–A67)

.....

Graduación

A52. La naturaleza y la extensión del conocimiento que se requiere es una cuestión de juicio profesional del auditor y varía de una entidad a otra en función de la naturaleza y las circunstancias de la entidad, incluido:

- la dimensión y la complejidad de la entidad, incluido su entorno de TI;
- la experiencia previa del auditor con la entidad;
- la naturaleza de los sistemas y procesos de la entidad, incluido si están o no formalizados, y

A55. 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.

NIA ES-SP 1315

División del control interno en componentes

.....

(c) el sistema de información, incluidos los procesos de negocio relacionados, relevantes para la información financiera, y la comunicación;

.....

Características de los elementos manuales y automatizados del control interno relevantes para la valoración del riesgo por el auditor

A53. El sistema de control interno de una entidad comprende elementos manuales y, a menudo, elementos automatizados. Las características de los elementos manuales o automatizados son relevantes para la valoración del riesgo por el auditor y para los procedimientos de auditoría posteriores basados en dicha valoración.

A54. La utilización de elementos manuales o automatizados en el control interno también afecta al modo en que se inician, registran y procesan las transacciones y se informa sobre ellas:

NIA-ES 315 R

.....

A108. La evaluación por el auditor del entorno de control en relación con la utilización de TI por la entidad puede incluir cuestiones tales como:

- Si la gobernanza sobre las TI es acorde con la naturaleza y complejidad de la entidad y de sus operaciones

A108. La evaluación por el auditor del entorno de control en relación con la utilización de TI por la entidad puede incluir cuestiones tales como:

- 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.

- 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 modificación)).

NIA ES-SP 1315

.....

- Los controles en los sistemas de TI consisten en una combinación de controles automatizados (por ejemplo, controles integrados en programas informáticos) y de controles manuales. Además, los controles manuales pueden ser independientes de las TI, pueden utilizar información producida por las TI, o pueden limitarse al seguimiento del funcionamiento efectivo de las TI y de los controles automatizados, así como al tratamiento de las excepciones. Cuando se utilizan las TI para iniciar, registrar, procesar o notificar transacciones u otros datos financieros, para su inclusión en los estados financieros, los sistemas y programas pueden incluir controles relacionados con las correspondientes afirmaciones en el caso de cuentas materiales o pueden ser decisivos para un funcionamiento eficaz de los controles manuales que dependen de las TI. La combinación por la entidad de elementos manuales y automatizados en su control interno varía según la naturaleza y complejidad de la utilización de las TI por la entidad.

NIA ES-SP 1315

A56. Las TI también originan riesgos específicos para el control interno de la entidad, incluidos, por ejemplo:

- La confianza en sistemas o programas que procesan datos de manera inexacta, que procesan datos inexactos, o ambos.
- Accesos no autorizados a los datos que pueden tener como resultado la destrucción de datos o cambios indebidos de ellos, incluido el registro de transacciones no autorizadas o inexistentes, o un registro inexacto de las transacciones.

Pueden producirse riesgos específicos cuando múltiples usuarios acceden a una misma base de datos.

- La posibilidad de que el personal del departamento de TI obtenga permisos de acceso más allá de los necesarios para realizar sus tareas, dejando así de funcionar la segregación de funciones.
- Cambios no autorizados en los datos de los archivos maestros.
- Cambios no autorizados en los sistemas o programas.
- No realizar cambios necesarios en los sistemas o programas.
- Intervención manual inadecuada.
- Pérdida potencial de datos o incapacidad de acceder a los datos del modo requerido.

NIA ES-SP 1315

El sistema de información, incluidos los procesos de negocio relacionados, relevante para la información financiera y la comunicación (Ref.: Apartado 18).

A81. El sistema de información financiera relevante para los objetivos de la información financiera, que incluye el sistema contable, comprende los procedimientos y registros diseñados y establecidos para:

- iniciar, registrar y procesar las transacciones de la entidad (así como los hechos y condiciones) e informar sobre ellas, así como para rendir cuentas sobre los activos, pasivos y patrimonio neto correspondientes;
- resolver el procesamiento incorrecto de transacciones, por ejemplo, ficheros de espera automatizados y procedimientos aplicados para reclasificar oportunamente las partidas pendientes de aplicación;
- procesar y dar cuenta de elusiones del sistema o evitación de los controles;
- transferir información desde los sistemas de procesamiento de las transacciones al libro mayor;
- capturar información relevante para la información financiera sobre los hechos y las condiciones distintos de las transacciones, tales como la depreciación y la amortización de activos, así como los cambios en la recuperabilidad de las cuentas a cobrar; y
- asegurar que se recoge, registra, procesa, resume e incluye adecuadamente en los estados financieros la información que el marco de información financiera aplicable requiere que se revele.

NIA ES-SP 1315

Riesgos derivados de las TI (Ref.: Apartado 21)

A95. La utilización de TI afecta al modo en que se implementan las actividades de control. Desde el punto de vista del auditor, los controles sobre los sistemas de las TI son eficaces cuando mantienen la integridad de la información y la seguridad de los datos que procesan dichos sistemas, e incluyen controles generales de las TI y controles de aplicaciones eficaces.

A96. Los controles generales de las TI son políticas y procedimientos vinculados a muchas aplicaciones y favorecen un funcionamiento eficaz de los controles de las aplicaciones. Son aplicables en entornos con unidades centrales, redes de trabajo y de usuarios finales. Los controles generales de las TI que mantienen la integridad de la información y la seguridad de los datos generalmente incluyen controles sobre lo siguiente:

- Centros de datos y operaciones de redes.
- Adquisición, reposición y mantenimiento de software de sistemas.
- Cambios en los programas.
- Seguridad de accesos.
- Adquisición, desarrollo y mantenimiento de aplicaciones.

NIA ES-SP 1315

El proceso de valoración del riesgo por la entidad

.....

4. Los riesgos relevantes para una información financiera .....

- Sistemas de información nuevos o actualizados. Los cambios rápidos y significativos en los sistemas de información pueden modificar el riesgo relativo al control interno.

- Nueva tecnología. La incorporación de nuevas tecnologías a los procesos productivos o a los sistemas de información puede cambiar el riesgo asociado al control interno.

.....

El sistema de información, incluidos los procesos de negocio relacionados, relevante para la información financiera, y la comunicación

5. Un sistema de información está constituido por una infraestructura (componentes físicos y de hardware), software, personas, procedimientos y datos. Muchos sistemas de información hacen un amplio uso de las tecnologías de la información (TI).

NIA ES-SP 1315

Condiciones y hechos que pueden indicar la existencia de riesgos de incorrección material

.....

- Incongruencias entre la estrategia de TI de la entidad y sus estrategias de negocio.
- Cambios en el entorno de las TI.
- Instalación de nuevos y significativos sistemas de TI relacionados con la información financiera.

.....

Factores de riesgo inherente relevantes:	Ejemplos de hechos o condiciones que pueden indicar la existencia de riesgos de incorrección material en las afirmaciones:
	TI: • Cambios en el entorno de las TI. • Instalación de nuevos y significativos sistemas de TI relacionados con la información financiera.

- *Utilización de TI*. Los riesgos relacionados con:
  - el mantenimiento de la integridad de los datos y del procesamiento de la información;
  - los riesgos para la estrategia de negocio de la entidad que se originan si la estrategia de TI de la entidad no sustenta eficazmente la estrategia de negocio de la entidad; o
  - cambios o interrupciones en el entorno de TI de la entidad, cambios de personal de TI o cuando la entidad no realiza las necesarias actualizaciones del entorno de TI o dichas actualizaciones no se realizan oportunamente.

Anexo 5

Consideraciones para el conocimiento de las Tecnologías de la Información (TI)

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

El sistema de control interno de la entidad contiene elementos manuales y automatizados .....

Las características de los elementos manuales o automatizados son relevantes para la identificación y valoración

En la obtención de conocimiento del entorno de TI relevante para los flujos de transacciones y el procesamiento

	Ejemplos de características habituales de:		
	Software comercial no complejo	Software comercial o aplicaciones de TI de tamaño medio y moderadamente complejos	Aplicaciones grandes o complejas (por ejemplo, sistemas de planificación de recursos (EPR))

Anexo 6

Consideraciones para el conocimiento de los controles generales de TI

(a) Aplicaciones

(b) Base de datos

(c) Sistema operativo

(d) Red

.....

(a) Proceso para gestionar el acceso:

(b) Procesos para la gestión de cambios en los programas o al entorno de TI.

(c) Proceso para la gestión de las operaciones de TI.

Anexo 6

Proceso	Riesgos	Controles	Aplicaciones de TI		
Proceso de TI	**Ejemplos de riesgos derivados de la utilización de TI**	**Ejemplos de controles generales de TI**	**Software comercial no complejo – Aplicable (sí/no)**	**Software comercial o aplicaciones de TI de tamaño medio y moderadamente complejos – Aplicable (sí/no)**	**Aplicaciones de TI de gran tamaño o complejas (por ejemplo, sistemas EPR) – Aplicable (sí/no)**
Gestión de acceso	Permisos de acceso de usuarios: Los usuarios tienen permisos de acceso más allá de los necesarios para realizar sus tareas, lo que puede dar lugar a una incorrecta segregación de funciones.	La dirección aprueba la naturaleza y la extensión de los permisos de acceso de usuarios para nuevos usuarios o modificaciones de los permisos existentes, incluidos perfiles/funciones estándar por aplicaciones, transacciones críticas	Sí – en vez de revisiones de acceso de usuarios mencionadas más abajo	Sí	Sí

Otros Marcos de referencia: ISACA

Guias generales y detallades de auditoria de STIC

Estandard internacional de auditoria STIC

Certificación internacional de Auditor SI – CISA –

COBIT

Otros Marcos de referencia: ISO27k

ISO 27001 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

.....Reducir los riesgos y proteger la información desde la perspectiva de confidencialidad, integridad y disponibilidad.

Secuencia de accionas organizativas y de gestión para establecimiento, implementación, operación, supervisión, revisión, mantenimiento y mejora del SGSI “ISMS (Information Security Management System)”.

.....

Conceptos y requisitos: ENS

Principios básicos

Proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema.

Detección, análisis y minimización de los riesgos constante.

Las medidas de prevención tienen por objetivo evitar incidencias; las de reacción, identificar y minimizar los daños; las de recuperación permiten restablecer la información afectada por la incidencia.

Conformadas por medidas organizativas, físicas y lógicas que en caso de incidencia, minimice los daños.

Las medidas de seguridad tienen que estar en constante revisión y actualización.

Hay que separar en diferentes personas al responsable de la información, al responsable de servicio y al responsable de seguridad.

Medidas de seguridad

El nuevo reglamento general no regula específicamente las medidas de seguridad que se tendrán que aplicar, sino que se limita a indicar que habrá que aplicar las medidas técnicas y organizativas adecuadas al riesgo que comporte el tratamiento, entre otros:

- ✓ Seudonimización y cifrado.
- ✓ Capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- ✓ Capacidad de restaurar la disponibilidad y el acceso a los datos de forma rápida en caso de incidente físico o técnico.
- ✓ Proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas.

Gracias por su atención

¿Ruegos y preguntas?

auren
A PROP TEU PER ARRIBAR LLUNY

AUREN ESPANYA
www.auren.es
Alacant - Barcelona - Bilbao - Cartagena - La Corunya - Las Palmas de Gran Canaria
Madrid - Màlaga - Múrcia - Palma - Saragossa - Sevilla - València - Valladolid - Vigo

AUREN INTERNACIONAL
www.auren.com
Alemanya - Argentina - Colòmbia - Mèxic - Països Baixos - Portugal - Uruguai - Xile

PRESÈNCIA EN ALTRES LLOCS DEL MÓN:

Membre de:

Antea
ALLIANCE OF INDEPENDENT FIRMS

www.antea-int.com