2024

Metodología común de inspección de auditoría

Programa de trabajo de inspección sobre auditoría de tecnologías de la información (TI)

Emitido por la Comisión de Órganos Europeos de Supervisión de Auditores (COESA/CEAOB en inglés)

Traducido por:

AUDITORES
INSTITUTO DE CENSORES JURADOS DE CUENTAS DE ESPAÑA

Glosario de abreviaturas empleadas en la traducción

ATT	Herramientas y técnicas automatizadas
CATI	Controles de aplicación en las tecnologías de la información
CGTI	Controles generales de tecnologías de la información
IPE	Información proporcionada/producida por la entidad
JET	Comprobación de entradas en el diario
RIM	Riesgo de incorrección material
TI	Tecnologías de la información

Traducido por:

AUDITORES
INSTITUTO DE CENSORES JURADOS
DE CUENTAS DE ESPAÑA

Principios clave	
PROGRAMA DE TRABAJO DE INSPECCIÓN SOBRE TI	
	El programa de inspección de auditoría de TI facilita la inspección del **trabajo sobre TI realizado por el auditor como parte de una auditoría de estados financieros.** Habitualmente, este trabajo sobre TI lo realizan especialistas en TI de la firma de auditoría.

Conclusiones clave	
Al finalizar los procedimientos relativos a esta área, evaluar como conclusión si:	
1	El equipo de inspección está satisfecho de que el auditor ha identificado y valorado adecuadamente los RIM derivados del entorno de control relevante de TI, así como los riesgos derivados de la utilización de TI.
2	El auditor obtuvo respuestas de auditoría a los RIM derivados del entorno de control relevante de TI suficientes y adecuadas, así como a los riesgos derivados de las TI.

Definiciones[1]	
Controles de acceso	Procedimientos diseñados para restringir el acceso a dispositivos on-line, programas y datos. Los controles de acceso consisten en la "autenticación de usuario" y "autorización de usuario". La "autenticación de usuario" normalmente intenta identificar un usuario a través de identificaciones únicas para comenzar la sesión, contraseñas, tarjetas de acceso o datos biométricos. La "autorización de usuario" consiste en reglas de acceso para determinar los recursos del ordenador a los que puede acceder cada usuario. De forma específica, estos procedimientos están diseñados para prevenir o detectar: (i) el acceso no autorizado a terminales, programas y datos electrónicos (on-line); (ii) el registro de transacciones no autorizadas; (iii) los cambios no autorizados en ficheros de datos; (iv) el uso de programas de ordenador por personal no autorizado; y (v) el uso de programas de ordenador que no han sido autorizados.
Controles de aplicación en las tecnologías de la información (CATI)	Procedimientos manuales o automatizados que operan habitualmente en relación con la gestión de procesos. Los controles de aplicación pueden ser de naturaleza preventiva o de detección y se diseñan para asegurar la integridad de los registros contables. Por consiguiente, los controles de aplicación están relacionados con los procedimientos que se usan para iniciar, registrar, procesar e informar sobre transacciones u otros datos financieros.
Herramientas y técnicas automatizadas	Mediante la utilización de herramientas y técnicas automatizadas, el auditor puede aplicar procedimientos de valoración del riesgo a un gran volumen de datos (del mayor, de los libros auxiliares o de otros datos operacionales) incluidos procedimientos de análisis, recálculos, reejecución o conciliaciones. El auditor puede utilizar herramientas y técnicas automatizadas para entender los flujos de transacciones y su procesamiento como parte de sus procedimientos para conocer el sistema de información. Un resultado de esos procedimientos puede ser que el auditor obtenga información sobre la estructura organizativa de la entidad o sobre las personas con las que hace negocios (por ejemplo, proveedores, clientes, partes vinculadas). Las herramientas y técnicas automatizadas también se pueden utilizar para observar o inspeccionar, en especial activos, por ejemplo, mediante el uso de herramientas de observación remota (por ejemplo, un dron).
Controles generales de TI (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 integridad, exactitud y validez de la información) en el sistema de información de la entidad. Los controles generales de TI son controles sobre los procesos de TI de la entidad. (El Anexo 6 de la NIA 315 proporciona ejemplos de CGTI).

1 Las definiciones de controles de acceso, controles de aplicación en las tecnologías de la información, técnicas de auditoría asistidas por ordenador, sistema de información relevante para la información financiera y organización de servicios se han extraído del glosario de términos incluido en el Volumen 1 del «Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros encargos de Aseguramiento y Servicios relacionados» del Consejo de Normas Internacionales de Auditoría y Aseguramiento, edición 2020. Las definiciones de controles generales de TI, controles de procesamiento, entorno de TI, riesgo derivado de la utilización de TI y sistema de control interno se han extraído de la NIA 315 (Revisada 2019).

Controles de 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).
Sistema de información relevante para la información financiera	Un componente del control interno que incluye el sistema de información financiera y que consiste en procedimientos y registros establecidos para iniciar, registrar, procesar e informar transacciones de la entidad (así como hechos y condiciones) y para mantener la rendición de cuentas sobre los activos, los pasivos y el patrimonio relacionados.
Entorno de 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: (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 o 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.
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).
Organizaciones de servicios	Organización externa (o segmento de una organización externa) que presta a las entidades usuarias servicios que forman parte de los sistemas de información relevantes para la información financiera de dichas entidades usuarias.
Evaluación del 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. El sistema de control interno consiste en 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, (v) las actividades de control.

Paso	Objetivo de la comprobación	Referencia	Procedimientos de inspección
Procedimientos de valoración del riesgo			
1	Evaluar si el auditor identificó y valoró adecuadamente los RIM derivados de la utilización de TI.	NIA 315, Apartados 19 y A56-A67, A140-A143 NIA 315, Anexo 5 NIA 600, Apartado 17 NIA 402, Apartado 14 NIA 402, Apartado 16 NIA 402 17 NIA 315, Apartados 21-26 y A108, A166-A174 NIA 315, Apartados 19 y A56-A67 NIA 300, Apartados 8 y A8 ; NIA 220, Apartado 14 NIA 200, Apartado 14 NIA 315, Apartados 19 y A56-A67 NIA 315, Apartados 26 y A150 y A158 NIA 620, Apartado 9 NIA 620, Apartados A14- A20 NIA 315, Apartado 19 NIA 315, Anexo 2 NIA 701, Apartados 9 y A18	1. Evaluar si el auditor obtuvo un conocimiento de la entidad y de su entorno y, en particular, la medida en la que el modelo de negocio integra la utilización de TI. 2. Evaluar si el auditor obtuvo un conocimiento de los componentes del sistema de control interno de la entidad al aplicar los procedimientos de valoración del riesgo. 3. Evaluar si el auditor determinó adecuadamente la necesidad de habilidades o conocimientos especializados en TI para valorar los riesgos derivados de la TI y para diseñar y aplicar procedimientos de auditoría para responder a dichos riesgos. 4. Revisar si el auditor identificó y valoró adecuadamente los riesgos derivados de la utilización de TI, incluida la determinación de si los riesgos identificados se consideran significativos, específicamente con relación a los sistemas de información relevantes para la información financiera. 5. Evaluar si el auditor identificó hechos inusuales en las TI (por ejemplo, la implementación de un sistema de TI crítico, incidentes de TI graves, cambios en la organización o gobierno de la TI, etc.), evaluar si el auditor ha valorado adecuadamente los riesgos relacionados.
2	Evaluar si el auditor diseñó e implementó respuestas adecuadas a los RIM derivados de la utilización de TI.	NIA 315, Apartados 26, A150 y A166-A172 NIA 315, Apartado 30 NIA 330, Apartados 5 y A1, NIA 330 Apartados 7 y A16 y NIA 330 Apartados 8 y A24 NIA 315, Apartados 26 y A173 y NIA 701, Apartados 9 y A18	1. Evaluar si el auditor diseñó los procedimientos adecuados para tratar las particularidades de la entidad auditada con relación a la TI y, en particular, los RIM derivados de la TI. 2. Cuando el auditor identificó hechos inusuales en las TI (por ejemplo, implementación de un nuevo sistema crítico de TI), evaluar si el auditor aplicó adecuadamente procedimientos para responder a los correspondientes riesgos. Si ello se consideró una Cuestión clave de la auditoría, revisar si se ha tratado adecuadamente en el informe de auditoría, así como en el informe adicional dirigido al comité de auditoría, y que la información revelada es adecuada.

Paso	Objetivo de la comprobación	Referencia	Procedimientos de inspección
Evaluación de los controles generales de TI (CGTI)			
2a	Asegurarse de que las comprobaciones cubrieron todos los sistemas críticos de TI, incluidos los localizados y/o gestionados por organizaciones de servicios. -	NIA 315, Apartado 21 NIA 315, Apartados 26, A150 y A166-174 NIA 330, Apartados 10 y A29 NIA 315, Apartado 21 NIA 315 , Apartados 26, A150 y A166-174 NIA 330, Apartados 10 y A29 NIA 315, Apartado 21 NIA 315 , Apartados 26, A150 y A166-174 NIA 330, Apartados 10 y A29 NIA 402, Apartado 14 NIA 402, Apartado 16 NIA 402, Apartado 17 NIA 330, Apartados 12 y A33	1. Revisar el trabajo realizado por los especialistas en TI **sobre el proceso de gestión de cambios** para asegurarse de que los sistemas críticos de TI y todos los correspondientes niveles (aplicaciones, bases de datos, sistemas operativos e infraestructura de red) formaron parte del alcance, los CGTI relativos a la **gestión del cambio** se han comprobado adecuadamente (a. diseño e implementación, 2. eficacia operativa) y que la conclusión sobre el diseño, implementación y eficacia operativa de los CGTI está en línea con los resultados de las pruebas. a. b. c. 2. Revisar el trabajo realizado por los especialistas en TI sobre **controles de acceso y seguridad** para asegurarse de que los sistemas críticos de TI y todos los correspondientes niveles (aplicaciones, bases de datos, sistemas operativos e infraestructura de red) formaron parte del alcance, los CGTI relativos a los **controles de acceso y seguridad** se ha comprobado adecuadamente (a. diseño e implementación, 2. eficacia operativa) y que la conclusión sobre el diseño, implementación y eficacia operativa de los CGTI está en línea con los resultados de las pruebas. a. b. c. 3. **Si es aplicable, en función del modelo de negocio y/o del tipo de controles sobre aplicaciones identificados por la auditoría financiera (por ejemplo, transferencia automatizada de datos operativos al sistema de contabilidad)**, revisar el trabajo realizado por los especialistas de TI sobre las operaciones de TI para asegurarse de que los sistemas críticos de TI y todos los correspondientes niveles (aplicaciones, bases de datos, sistemas operativos e infraestructura de red) formaron parte del alcance, los CGTI relativos a las **operaciones de TI** se han comprobado adecuadamente (a. diseño e implementación, 2. eficacia operativa) y que la conclusión sobre el diseño, implementación y eficacia operativa de los CGTI está en línea con los resultados de las pruebas. a. b. c. 4. Para sistemas localizados y/o gestionados por organizaciones de servicios, revisar el trabajo realizado por los especialistas en TI sobre los controles realizados por terceros (en su caso). En particular, a. considerar el tipo de informe de terceros para conocer si se cubre la eficacia operativa y no solo el diseño e implementación de controles; b. evaluar el informe y considerar si el alcance de los procedimientos de auditoría aplicados por la organización de servicios del auditor responde a los riesgos identificados («no hay brecha») y considerar si la entidad está cubierta; c. considerar el periodo cubierto por los informes de terceros e identificar si la organización de servicios ha emitido una *carta puente*; d. evaluar las deficiencias informadas y los controles compensatorios, y evaluar su impacto potencial sobre los estados financieros; e. Verificar que el equipo de auditoría cubrió los «Controles complementarios de la entidad usuaria», es decir, los controles que la organización de servicios espera que la entidad usuaria ejecute de manera completa, adecuada y oportuna.
Evaluación de los controles de aplicación en las TI (CATI)			
2b	Asegurarse de que el auditor evaluó los controles relevantes del procesamiento de información / Controles de aplicación de las TI con un enfoque	NIA 315, Apartado 21 NIA 315, Apartados 26 y A166-181 y Anexo 5 NIA 330, Apartados 10 y A29-A31	1. Revisar la lista de controles de procesamiento, controles automatizados y/o controles que dependen de las TI seleccionados por el auditor, el enfoque adoptado para evaluar dichos controles y revisar si se ha llevado a cabo el trabajo adecuado (por ejemplo, pruebas sobre el diseño e implementación de los controles y su eficacia operativa) que fundamente las conclusiones sobre dichos controles. 2. Evaluar si los sistemas que incorporan los CATI relevantes han sido cubiertos por la evaluación de los CGTI y si se ha considerado la conclusión sobre los CGTI referentes a las CATI.

	adecuado.		
Evaluación de información relevante proporcionada por la entidad (IPE)			
2c	Evaluar si el auditor evaluó la fiabilidad de la información generada por los sistemas, por ejemplo, los informes relevantes.	NIA 315, Apartados 26 y A169; NIA 500, Apartado 7 NIA 500,Apartados 9 y A50-A51 NIA 330, Apartados 10 y A29-A31	1. Revisar la lista de información generada por el sistema, por ejemplo, informes utilizados por el auditor, el enfoque adoptado para evaluar la fiabilidad de esos informes (integridad y exactitud) y asegurarse de que se ha llevado a cabo el trabajo adecuado para fundamentar la conclusión sobre la fiabilidad de esos informes.
Paso	**Objetivo de la comprobación**	**Referencia**	**Procedimientos de inspección**
	(Producidos por sistemas de TI)		2. Evaluar si los sistemas que generan IPE han sido cubiertos por la evaluación de los CGTI y que se ha considerado la conclusión sobre los CGTI con relación a la IPE.
Fundamento de la comprobación de entradas en el diario (JET)			
2d	Asegurarse de que el trabajo de TI sobre las entradas en el diario sustenta adecuadamente el enfoque de auditoría para responder al riesgo de fraude.	NIA 500, Apartado 7 NIA 500, Apartados 9 y A50-A51; NIA 240, Apartados 33 y A42-A45	1. Cuando se aplica un enfoque de análisis de datos basado en ATT o se ha aplicado analítica de datos para la comprobación de las entradas en el diario, evaluar los procedimientos aplicados por el equipo del encargo con objeto de validar la integridad y exactitud de los datos electrónicos para comprobar las entradas en el diario. 2. Revisar las pruebas sobre las entradas en el diario para asegurarse de que son adecuadas y suficientes teniendo en cuenta el entorno y los factores de riesgo.
Utilización de herramientas y técnicas automatizadas (ATT)			
2e	Asegurarse de que el trabajo con ATT y/o las propias herramientas y técnicas automatizadas tiene su base en datos fiables, ha sido ejecutado correctamente y está suficientemente documentado.	NIA 330, Apartados7 y A16; NIA 500, Apartado 7 NIA 500, Apartados 9 y A50-A51; NIA 230, Apartado 8 NIA 315, Apartados 14 y A27–A31	1. Evaluar si los procedimientos para validar datos proporcionan el suficiente confort acerca de la integridad y exactitud de los datos utilizados por las ATT y/o las propias herramientas y técnicas automatizadas. 2. Revisar si la documentación del trabajo realizado con ATT para la evaluación es suficiente para comprender el modo en que se realizaron las pruebas y evaluar la utilización correcta de las ATT con relación a los objetivos del auditor. 3. Con relación a los procedimientos de valoración del riesgo, evaluar si las herramientas que sustentan los procedimientos analíticos, en particular cuando son automatizadas, se utilizaron correctamente.
Valoración general			

3	Revisar el modo en el que el auditor utilizó los resultados de los especialistas de TI	NIA 265, Apartado 9 NIA 315, Apartado 38 NIA 620, Apartados 12-13	**Procedimientos de inspección esperados:** 1. Evaluar si el auditor determinó adecuadamente que el trabajo de auditoría de TI realizado por los especialistas de TI es adecuado y está documentado para su finalidad. 2. Evaluar si el auditor ha investigado y tratado adecuadamente los hallazgos significativos surgidos, en particular, los relacionados con CGTI y CATI, y si han sido comunicados a la entidad auditada.

Recursos adicionales	
ISACA	Marco COBIT, Cybersecurity Nexus, conocimiento IT (https://www.isaca.org/)
ISO	Serie ISO/IEC 2700x (https://www.iso.org/
ITIL	Information Technology Infrastructure Library (ITIL)
NIST	Inteligencia artificial, Tecnología de la información, ciberseguridad (https://www.nist.gov/)
BSI	BSI (Oficina Federal de Seguridad de la Información) (https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html)
GDPR	GDPR (Reglamento general de protección de datos (EU) 2016/679) (https://en.wikipedia.org/wiki/General_Data_Protection_Regulation)