ISSAI 5300

Las Normas Internacionales de las Entidades Fiscalizadoras Superiores, o ISSAI, son emitidas por la INTOSAI, la Organización Internacional de las Entidades Fiscalizadoras Superiores. Para obtener más información, visite *www.issai.org*

INTOSAI

Directrices sobre Auditoría de TI

Junio de 2016

Comité de Normas Profesionales de la INTOSAI

Secretaría del PSC

Rigsrevisionen • Landgreven 4 • P.O. Box 9009 • 1022 Copenhagen K • Dinamarca

Tel.:+45 3392 8400 • Fax: +45 3311 0415 • E-mail: info@rigsrevisionen.dk

I N T O S A I

Secretaría General de la INTOSAI - RECHNUNGSHOF

(Tribunal de Cuentas de Austria)

DAMPFSCHIFFSTRASSE 2

A-1033 VIENA

AUSTRIA

Tel .: ++ 43 (1) 711 71 • Fax: ++ 43 (1) 718 09 69

E-MAIL: intosai@rechnungshof.gv.at;

WORLD WIDE WEB: http://www.intosai.org

Tabla de Contenidos

PREFACIO

La serie 5300-5399 de las ISSAI ha sido asignada a las Directrices sobre Auditoría de Tecnología de la Información en el marco de estas normas internacionales. La ISSAI 5300, primera en la serie ISSAI 5300, es de alcance global y contiene principios generales sobre los fundamentos de la auditoría de TI. Aborda los principios, el enfoque y la metodología general para realizar este tipo de auditorías.

La ISSAI 5300 también tiene busca servir como una guía para que las EFS puedan llevar a cabo auditorías de TI, desarrollar la capacidad de auditoría de TI y utilizar los recursos limitados de auditoría de TI, a fin de proporcionar una garantía a las entidades auditadas, al gobierno y al pueblo de un país en materia de integridad, confiabilidad y relación precio-calidad en implementaciones de TI.

La ISSAI 5300 se ha desarrollado en el marco de las ISSAI, mediante la realización de una revisión de las normas existentes en relación con las auditorías de TI/Auditorías de Sistemas de Información, las normas relativas a los sistemas de información, las normas nacionales e internacionales de auditoría, en particular, las ISSAI existentes. Otra característica clave de la ISSAI 5300 es que asegura que la naturaleza básica inherente a las auditorías de TI esté vinculada/integrada adecuadamente, con las diferentes formas de auditoría identificadas en las ISSAI nivel 3.

Además, al ser una orientación nivel 4, el material en esta ISSAI se ha dividido en dos categorías: **Requisitos** - elementos esenciales para la realización de una auditoría de TI de buena calidad; seguido por **Explicaciones** - que interpretan y definen los requisitos en términos más generales. Esto se ha hecho para asegurar que la ISSAI conserve su función principal de proporcionar orientación y apoyo general como está previsto en el marco de las ISSAI.

La ISSAI 5300 también tiene en cuenta los niveles de madurez de los sistemas de información en el sector gubernamental y el nivel de madurez de las auditorías de TI en diferentes EFS.

Esta ISSAI se estructura en los siguientes subtemas principales:

1. Marco para las auditorías de TI;
2. Requisitos generales específicamente relacionados con las auditorías de TI;
3. Requisitos específicos para el proceso de auditoría de TI;
4. Técnicas y herramientas de auditoría de TI;
5. Requisitos de información de las auditorías de TI.

Es importante destacar que existe un anexo dedicado al análisis de datos.

Esta ISSAI sienta las bases para el desarrollo futuro de las ISSAI de la serie 5300-5399 y/o de guías sobre materias específicas, de interés para la comunidad de la INTOSAI en el ámbito de las auditorías de TI.

La elaboración de este trabajo estuvo a cargo de un equipo compuesto por las EFS de Brasil, India (jefe de proyecto), Indonesia, Japón, Polonia y los EE.UU, EFS que estuvo a cargo de su redacción.

A. MARCO PARA LA AUDITORÍA DE TI

1. Mandato y alcance de la ISSAI 5300

1.1 La ISSAI 5300 establece el marco general para la realización de las auditorías de TI en el marco de las ISSAI.

1.2 El marco establecido en esta ISSAI es coherente con los Principios Fundamentales de la Auditoría del Sector Público (ISSAI 100), los Principios Fundamentales de la Auditoría Financiera (ISSAI 200), los Principios fundamentales de la Auditoría de Desempeño (ISSAI 300) y los Principios Fundamentales de la Auditoría de Cumplimiento (ISSAI 400).

1.3 Este proyecto de ISSAI define los requisitos para la práctica profesional de la auditoría de TI, seguido de explicaciones para mejorar la claridad y facilidad de lectura del marco.

1.4 Los requisitos contienen información necesaria para un trabajo de alta calidad en materia de auditoría de TI. Estos permiten que los auditores sepan lo que se espera de ellos y que los grupos de interés sepan lo que pueden esperar de la auditoría de TI realizada por una EFS.

1.5 Las explicaciones describen con más detalle lo que significa un requisito o lo que intenta abarcar.

1.6 Este proyecto de ISSAI ha sido preparado por un equipo de proyecto compuesto por las EFS de Japón, Polonia, Indonesia, India, los EE.UU. y Brasil.

2. Introducción a las Auditorías de TI

2.1 Las entidades gubernamentales han adoptado cada vez más las tecnologías de la información y la comunicación (TIC) para llevar a cabo sus funciones y ofrecer diversos servicios. Tales sistemas basados en las TIC son comúnmente conocidos como Sistemas de Información (SI) o Sistemas de Tecnología de la Información (TI).

2.2 Las Entidades Fiscalizadoras Superiores (EFS) tienen el mandato de auditar al Gobierno y sus entidades, de acuerdo con su respectivo mandato de auditoría.[1]

2.3 Las EFS, por lo tanto, promueven la eficiencia, la rendición de cuentas, la eficacia y la transparencia de la administración pública[2].

2.4 El desarrollo continuo de la tecnología de la información y la comunicación ha hecho posible capturar, almacenar, procesar y entregar información en forma electrónica. Esta transición hacia el procesamiento electrónico ha provocado un cambio significativo en el entorno en el que trabajan las EFS. Por otra parte, el gasto del gobierno en TI está creciendo, por lo tanto se hace imperativo para las EFS desarrollar la capacidad adecuada para llevar a cabo las auditorías de TI.

3. Definición de auditoría de TI

3.1 Las auditorías de TI se definen como:

"Un examen y revisión de los sistemas de TI y controles relacionados que busca aumentar la seguridad o identificar violaciones a los principios de legalidad, eficiencia, economía y eficacia del sistema de TI y sus controles relacionados."

3.2 Auditoría de TI[3] es por lo tanto, un término amplio que abarca las auditorías financieras[4] (para evaluar la exactitud y el cumplimiento de las declaraciones realizadas en los estados

[1] ISSAI 1, Declaración de Lima
[2] Resolución de la Asamblea General de las Naciones Unidas A/66/209
[3] La auditoría de TI también se conoce como auditoría de SI, auditoría de sistemas, auditoría de la información, auditoría de seguridad de la información, revisión de aseguramiento informático, aseguramiento de TI, etc.
[4] ISSAI 200 Principios Fundamentales de la Auditoría Financiera

financieros de una organización), las auditorías de cumplimiento[5] (evaluación de los controles internos), y las auditorías de desempeño[6] (para evaluar si los sistemas de TI satisfacen las necesidades de los usuarios y no someten a la entidad a riesgos innecesarios). Sin embargo, puede haber casos en que algunas auditorías sólo se destinen a evaluar un determinado componente TI de un sistema.

4. Mandato para las auditorías de TI

4.1 El mandato de la EFS para ejecutar auditorías de TI se deriva del mandato general entregado a la EFS para realizar auditorías.[7] Algunas EFS también pueden tener un mandato específico para la realización de auditorías de TI o auditoría de los sistemas de TI.

4.2 Para muchas EFS, el mandato para realizar auditorías financieras, auditorías de desempeño, y auditorías de cumplimiento será mandato suficiente para llevar a cabo las auditorías de TI. Esto se debe a que los sistemas de TI apoyan las principales operaciones de una entidad, las que pueden incluir los sistemas financieros. Por lo tanto, la ejecución de auditorías de TI puede no requerir mandatos adicionales.

4.3 El mandato específico, si se proporciona, debe definir el alcance de la auditoría para auditar sistemas de TI, que son utilizados por la entidad para cumplir sus objetivos funcionales. También debe proporcionar un acceso oportuno, ilimitado, directo y libre a todos los documentos necesarios y la información de la entidad[8], tanto físicos como electrónicos, ya sea si la función o cualquiera de su partes es realizada por personal interno o subcontratado.

4.4 El mandato de la EFS para llevar a cabo las auditorías de TI debe ajustarse a los principios contenidos en las ISSAI de los niveles 1 y 2.

B. REQUISITOS GENERALES ESPECÍFICAMENTE RELACIONADOS CON LAS AUDITORÍAS DE TI

5. Enfoque de auditoría basada en riesgos de la Auditoría de TI

Requisito:

El auditor deberá considerar los riesgos de la auditoría de TI cuando tome un riesgo basado en el enfoque, método o modelo de auditoría.

Las auditorías de TI deberán llevarse a cabo sobre la base de un enfoque de auditoría basada en riesgos

Explicación:

5.1 El enfoque de auditoría basada en riesgos implica la identificación de los elementos[9] de riesgo en la entidad que está siendo evaluada junto con su impacto potencial y, por lo tanto, la identificación de áreas prioritarias a ser auditadas.

5.2 Los riesgos presentes durante la realización de la auditoría de una entidad, implican riesgos inherentes, de control y la detección de estos. Los elementos del riesgo se identifican abordando los tres riesgos mencionados. Juntos, éstos constituyen lo que se llama el riesgo de auditoría.

---

[5] ISSAI 400 Principios Fundamentales de la Auditoría de Cumplimiento

[6] ISSAI 300 Principios Fundamentales de la Auditoría de Desempeño

[7] Principio 3, ISSAI 10 - Declaración de México sobre la Independencia de las EFS y las ISSAI 100 - Principios fundamentales de la Auditoría del Sector Público

[8] Acceso sin restricciones a los registros; Principio 4, ISSAI 10 - Declaración de México sobre la independencia de las EFS

[9] Los elementos de riesgo estarían relacionados con áreas como gobernanza de TI, diseño y desarrollo del sistema, contratación interna/externa, las operaciones, seguridad TI, monitoreo y control.

5.3 Los riesgos inherentes son aquellos que forman parte del sistema y que pueden tener impacto sobre el cumplimiento del mandato encomendado a la entidad. El anonimato de los usuarios es un riesgo inherente de un sistema de TI, especialmente en un entorno interconectado. Las organizaciones deberían establecer medidas de control para abordar los riesgos inherentes. En algunos casos, la entidad puede incluso aceptar los riesgos como tal - sin ningún tipo de medidas de respuesta para hacerles frente - cuando se determina que su impacto no es significativo y, por tanto, está dentro de un nivel de riesgo aceptable.

5.4 Los riesgos de control son aquellos donde las medidas de control pueden eventualmente fallar. En tales casos, es posible que surjan errores materiales, los que deberían ser identificados inmediatamente. Los sistemas de TI siempre abordan estos a través de Controles de Aplicación[10] y Controles Generales[11]. Es la robustez de estos controles lo que garantiza el cumplimiento de la función propia de la organización/sistema de TI. El fracaso o la puesta en peligro de estos controles constituyen una situación de de riesgos de control.

5.5 La detección de riesgos en la realización de las auditorías de TI dice relación con los riesgos de no detección, ausencia o falla de TI y sus controles relacionados, así como la puesta en riesgo asociada con el funcionamiento del sistema de TI.

5.6 Existen muchos enfoques de evaluación de riesgos y metodologías disponibles que la EFS puede elegir. Estas van desde simples clasificaciones del perfil de riesgo de los sistemas de TI como alto, medio y bajo, basándose en el criterio de los auditores TI de una EFS, a cálculos complejos y, aparentemente científicos que proporcionan una calificación de riesgos numérica de los sistemas de TI.[12]

6. Materialidad

Requisito:

La EFS deberá considerar la materialidad en todas las etapas del proceso de auditoría de TI.

Explicación:

6.1 Los auditores de TI deberán considerar la materialidad durante todo el proceso de auditoría (TI). Se debe tener en consideración que las consideraciones referentes a la materialidad afectan las decisiones que dicen relación con la naturaleza, oportunidad y alcance de los procedimientos de auditoría, así como la evaluación de los resultados de la auditoría. Las consideraciones pueden incluir las preocupaciones de las partes interesadas, el interés público, los requisitos reglamentarios y las consecuencias para la sociedad.[13]

6.2 La materialidad se refiere a todos los aspectos de estas auditorías, tales como la selección de los temas, la definición de los criterios, la evaluación de las pruebas y la documentación, así como también la gestión de los riesgos, cuestiones que influyen en un inadecuado o bajo impacto de las conclusiones o informes de auditoría.

---

[10] Los controles de aplicación son los controles incorporados en una aplicación individual o un grupo de aplicaciones relacionadas que comprenden un sistema de aplicación de TI. Estos poseen controles de entrada, controles de procesos, controles de salida y controles de datos maestros que son aplicables a la entrada, proceso y salida del sistema de TI.

[11] Los controles generales son controles sobre los sistemas y procesos relacionados que apoyan el sistema de aplicación de TI. Estos se refieren a áreas como la razón comercial del sistema de TI, diseño y desarrollo de sistemas, adquisiciones, contratación externa/interna, las operaciones (aparte de los controles de aplicación), gestión de recursos humanos, seguridad de TI, monitoreo, etc. Los controles generales y los controles de aplicación están asociados íntimamente, asegurando al mismo tiempo la implementación exitosa de un sistema informático. Si los controles generales son débiles, disminuyen considerablemente la fiabilidad de los controles asociados con las aplicaciones de TI individuales.

[12] Manual WGITA-IDI sobre auditorías de TI para Entidades Fiscalizadoras Superiores.

[13] ISSAI 100 - Principios Fundamentales de la Auditoría del Sector Público - Párrafo 41.

6.3 La materialidad de una auditoría de TI debería ser decidida bajo el marco general de una decisión a nivel de EFS. La perspectiva de la materialidad variará dependiendo de la naturaleza de la auditoría de TI. La materialidad relativa a auditorías financieras, de desempeño y cumplimiento del sector público, de las cuales las auditorías de TI forman parte, se discute en las ISSAI 200, 300 y 400[14].

6.4 Materialidad y Riesgo

La evaluación de riesgos utilizada en la auditoría de TI está íntimamente ligada a la materialidad de requisitos relativos a los intereses de las auditorías. La materialidad de un incumplimiento se evalúa con base en la capacidad de influir en las decisiones de los usuarios del sistema. Cuando los riesgos inherentes son altos, la aparición de un pequeño incumplimiento puede ser significativo debido a la posibilidad de que el efecto de tal incumplimiento posea una naturaleza acumulativa. Cuando los riesgos de control son altos (es decir, existe ausencia/falla de los controles necesarios para los riesgos identificados), de manera similar, un pequeño incumplimiento será significativo por la posibilidad de que el efecto de tal incumplimiento posea una naturaleza acumulativa.

6.5 Los auditores de TI no están siempre en condiciones de examinar todas las instancias / transacciones / módulos o sistemas, dadas las limitaciones de recursos y el costo-beneficio del ejercicio de auditoría. En tal situación, los auditores de TI pueden recurrir a la identificación de la materialidad y la adopción del muestreo de auditoría para un examen detallado, a fin de sacar conclusiones de auditoría razonables. Se puede recurrir al uso de herramientas de TI en la realización de diferentes tipos de muestreo. Los niveles de riesgos inherentes y de riesgos de control pueden impactar en el tamaño de la muestra. A mayor riesgo inherente o riesgo de control, mayor debiese ser el tamaño de la muestra.

7. Documentación

Requisito:

La EFS mantendrá suficiente documentación del proceso de auditoría de TI y sus resultados para garantizar que cualquier auditor experimentado ajeno a la auditoría pueda replicarla.

El auditor deberá preparar una documentación de auditoría que sea completa y detallada a fin de proporcionar una comprensión global de la auditoría.

La revisión de la documentación debe permitirle a cualquier otro auditor de TI llegar a las mismas conclusiones de la auditoría.

Explicación:

7.1 Los requisitos generales de documentación en una auditoría de TI son esencialmente aquellos descritos en las ISSAI de nivel 3, a saber: ISSAI 100, 200, 300 y 400. Estos también se aplicarían a una auditoría de TI. Sin embargo, la naturaleza de las auditorías de TI puede necesitar ajustes específicos en el proceso de documentación.

7.2 El rol de la documentación en una auditoría de TI es permitir comprender la planificación y ejecución de la auditoría, que trabajo se llevó a cabo en apoyo de los hallazgos y conclusiones, y en la elaboración de las recomendaciones de la auditoría. La documentación debe ser lo suficientemente detallada como para permitir que un auditor de TI con experiencia, sin conocimiento previo de la auditoría, entienda la naturaleza, oportunidad, alcance y resultados de los procedimientos realizados de conformidad con las ISSAIs pertinentes, normas nacionales y requisitos legales y reglamentarios aplicables. La evidencia obtenida, que sirve de apoyo a las conclusiones y recomendaciones de la auditoría, al razonamiento detrás de todas las materias importantes que requieren el ejercicio de un juicio profesional y las consiguientes conclusiones, también deben ser

[14] ISSAI 200 - Principios Fundamentales de la Auditoría Financiera, ISSAI 300 - Principios Fundamentales de la Auditoría de Desempeño, ISSAI 400 - Principios Fundamentales de la Auditoría de Cumplimiento.

documentadas, de modo que sea fácil de entender por un auditor de TI con experiencia. La documentación debe ser fiable, de manera que no exista desacuerdo sobre el contenido de la documentación con la entidad auditada.

7.3 La documentación en una auditoría de TI juega un papel importante para asegurar que cada paso del proceso de auditoría y cada hallazgo sea mapeado o referenciado a un punto específico del cumplimiento o incumplimiento de las normas o regulaciones aplicables.

7.4 Al igual que en cualquier otra auditoría, si cualquier hallazgo en el transcurso de una auditoría no es coherente con la conclusión general de la auditoría relativa a una materia importante o hay un desacuerdo con la entidad auditada sobre las conclusiones de la auditoría, entonces, los auditores de TI tienen que documentar la forma en que han abordado aquella inconsistencia y/o desacuerdo.

7.5 Formato de la documentación de auditoría de TI

La documentación de la auditoría de TI incluye formatos de papel y plantillas electrónicas para registrar información sobre el sistema de TI auditado, los detalles de las reuniones mantenidas con la dirección y dentro del equipo de auditoría, los hallazgos de auditoría, y las pruebas de las conclusiones de la auditoría. No hay un formato estándar para la documentación de la auditoría de TI en las ISSAI. Por lo demás, los formatos pueden diferir entre las diferentes EFS. Es posible que haya cierto grado de estandarización dentro de cada EFS en términos de checklists, modelos, organización de papeles de trabajo, etc.

7.6 Resguardo de la documentación de auditoría de TI

La documentación de auditoría de TI debe ser resguardada y protegida de cualquier modificación y eliminación no autorizada. Cada EFS puede desarrollar nuevas normas para el resguardo de la documentación de auditoría de TI o adaptar las normas existentes para satisfacer los requisitos de conservación de la documentación relativa a auditoría de TI. El período de almacenamiento así definido, sería una función del mandato de la EFS individual y del estatuto(s) que rige sus actividades.

Se debe prestar especial atención a los medios de comunicación, el formato, la vida útil y los requisitos de almacenamiento de estos datos, para asegurar que estos sean legibles dentro del plazo definido en la respectiva política de almacenamiento y retención de datos de cada EFS. Esto puede requerir la conversión de los datos de un formato a otro para mantenerse al día con los avances tecnológicos y la obsolescencia.

8. Competencia

Requisito:

La EFS deberá asegurarse de que el equipo de auditoría esté compuesto por miembros que poseen colectivamente las competencias para realizar la auditoría de TI de acuerdo con las normas.

Explicación:

8.1 Los conocimientos, habilidades y competencias necesarias podrían adquirirse a través de una combinación de capacitación, selección de personal nuevo y contratación de recursos externos de acuerdo con el plan estratégico de la EFS.

C. REQUISITOS RELACIONADOS CON EL PROCESO DE AUDITORÍA DE TI

9. Planificación de auditorías de TI

Requisito:

La EFS debe planificar una auditoría de TI basada en la evaluación de riesgos.

Explicación:

9.1 La planificación de la Auditoría de TI por parte de una EFS, puede llevarse a cabo de acuerdo con los mandatos legislativos, solicitudes legislativas / ejecutivas, o por iniciativa propia.

9.2 Planificación de auditoría en las EFS basada en la evaluación de riesgos

Las EFS pueden planificar auditorías basada en la evaluación de riesgos. En este proceso la EFS prioriza y selecciona las auditorías que se llevarán a cabo, sobre la base de una evaluación de riesgos. La planificación de una auditoría de TI basada en el riesgo se puede llevar a cabo en tres niveles - Estratégico, Anual, y de Equipo, los que estarán sujetos al plan estratégico general de la EFS. Sin embargo, una EFS puede decidir por una mezcla de uno o más de estos niveles, como por sus recursos y requisitos de auditoría, basados en el análisis de riesgo.

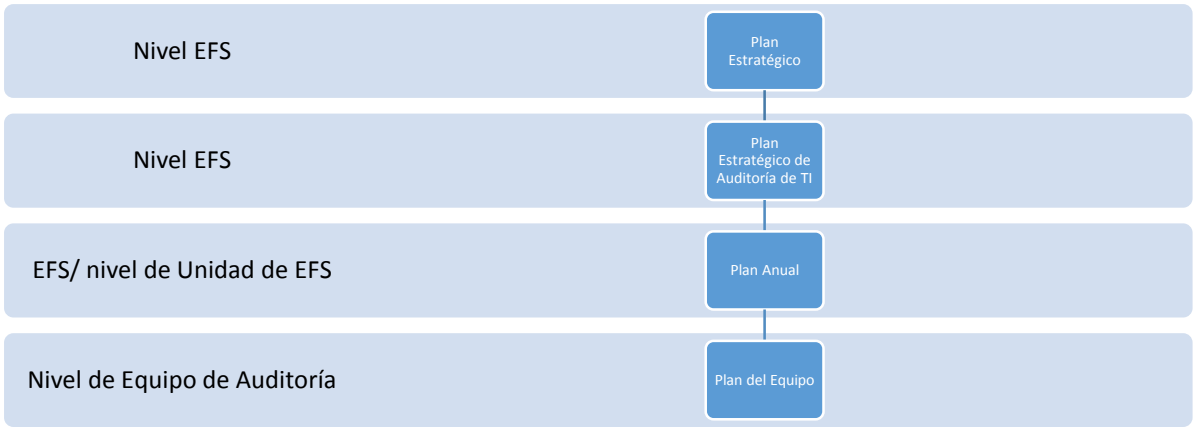

Figura 1: JERARQUÍA DE PLANIFICACIÓN DE AUDITORÍA TÍPICA PARA LAS EFS

10. Planificación estratégica de auditoría de TI

Requisito:

El plan estratégico de una EFS deberá poseer un componente que oriente la auditoría de TI y sus requerimientos asociados.

La EFS deberá desarrollar el Plan estratégico de auditoría de TI de acuerdo con el plan estratégico general de auditoría.

Explicación:

10.1 El plan estratégico de auditoría de TI contiene las metas y los objetivos de la auditoría de los sistemas de TI en las entidades gubernamentales sometidas al control de una EFS. El plan se determina normalmente por un período de entre 3-5 años, reflejando la evolución del entorno de TI y su adopción por parte de las entidades gubernamentales. El plan estratégico para la auditoría de los sistemas de TI debe estar alineado con el plan estratégico general de la EFS.

10.2 Las EFS tienen por objetivo garantizar la transparencia, la rendición de cuentas y la contribución a la buena gobernanza, en consonancia con su visión, misión y valores. Como tal, su plan estratégico u objetivos deberían abordar el desarrollo institucional, el desarrollo del sistema organizacional y el desarrollo de la capacidad profesional, según sea necesario, en respuesta a la consecución de sus metas estratégicas. Para las auditorías de TI, las EFS pueden evaluar su entorno a través de encuestas, la interacción con las entidades auditadas, la evaluación de la dirección y el desarrollo de soluciones tecnológicas y sus adopciones por parte de las entidades auditadas, y cualquier otro requisito legal u obligatorio.

10.3 La identificación del universo de auditoría en esta etapa será relevante. Las EFS podrán identificar sus prioridades de auditoría en respuesta a la evaluación de su entorno y el universo de auditoría, y decidir sobre sus metas y objetivos estratégicos. Para lograr sus objetivos generales, a través de los medios y recursos limitados disponibles, el plan de implementación estratégica de la

EFS puede incluir la identificación de las necesidades relacionadas con el desarrollo institucional, lo que considerará el mandato y el marco legal que permiten a la EFS la realización de auditorías de TI, el desarrollo de sistemas organizacionales para establecer sistemas y procedimientos en la EFS, a fin de llevar a cabo las auditorías de TI y el desarrollo de la capacidad profesional para adquirir las habilidades y capacidades necesarias para poder llevar a cabo las auditorías de TI.

10.4 Planificación de auditoría basada en riesgos

La planificación de auditoría basada en riesgos implica abordar los elementos de riesgo que tendrán impacto sobre la pertinencia de las auditorías y la corrección de las conclusiones de auditoría elaborados como resultado de la misma. La evaluación del riesgo a nivel de planificación estratégica de auditoría de TI aborda la cuestión de la relevancia de las auditorías de TI con respecto al objetivo estratégico global de las EFS, ello con el objetivo de asegurar la buena gobernanza, la transparencia y la rendición de cuentas en la gestión pública.

10.5 Debe haber una revisión periódica y actualización del plan estratégico de la EFS para abordar aquellos objetivos que digan relación con garantizar la transparencia, la rendición de cuentas y la contribución a la buena gobernanza.

10.6 Se puede hacer referencia a las ISSAI, especialmente, a la ISSAI 100 - Principios Fundamentales de Auditoría del Sector Público - para abordar las cuestiones relacionadas con la planificación estratégica de una EFS.

11. Planificación anual de auditoría de TI

Requisito:

El plan anual de auditoría de TI debe estar de acuerdo con el plan estratégico de auditoría de TI.

El plan anual de auditoría de TI debe cubrir los asuntos de importancia incluidos en el plan estratégico de auditoría de TI de acuerdo con la prioridad determinada a través de la evaluación de riesgos.

Explicación:

11.1 La elaboración del plan anual de auditoría de TI debe estar alineado con el plan estratégico de auditoría de TI. Esta etapa de la planificación implica la selección del sistema de TI o entidad a ser auditada.

11.2 En el marco del plan estratégico de auditoría de TI de una EFS, se puede utilizar un enfoque basado en riesgos para priorizar y seleccionar los temas adecuados. Esto implicará la creación y uso de un inventario de organizaciones / sistemas de TI auditables, junto con criterios claves para llevar a cabo la evaluación de riesgos. Este inventario podría ser también el universo de auditoría identificado durante la etapa de Planificación Estratégica, pero con detalles específicos sobre el tipo y la descripción de los sistemas de TI /entidades a ser utilizados en la evaluación de su perfil de riesgo. Un marco de evaluación de riesgos desarrollado por las EFS puede utilizarse posteriormente para finalizar una selección de auditoría.

11.3 Además de un enfoque basado en el riesgo en la selección de los temas de auditoría, muchas EFS asumen auditorías por mandato de la ley y por solicitudes de los órganos de control (Congreso, Parlamento, etc.) o el Ejecutivo.

12. Planificación a nivel de equipo de auditoría de TI para auditorías seleccionadas

Requisito:

El plan de auditoría de TI a nivel de equipo deberá estar de acuerdo con la evaluación de riesgos en el plan anual de auditoría de TI.

El plan de auditoría de TI a nivel de equipo deberá cubrir las materias de las áreas de riesgo significativo identificadas en el plan anual de auditoría de TI e incluir un programa detallado de auditoría.

Explicación:

12.1 Este nivel implica el desarrollo de un programa de auditoría detallado, comenzando con la descripción de los objetivos de una auditoría de TI seleccionada.

12.2 El requisito previo para el desarrollo del programa de auditoría es tener un conocimiento acabado de la entidad auditada, sus sistemas de información y de TI, y sus actividades relacionadas.

12.3 El grado de conocimiento de la entidad y sus procesos que requieran los auditores de TI será determinado por la naturaleza de la entidad y el nivel de detalle con el que se está realizando el trabajo de auditoría. El objetivo o el propósito detrás de la implementación de un sistema de TI deben ser identificados. El conocimiento de la entidad debería incluir el negocio, los riesgos financieros e inherentes a los que se enfrenta la entidad y sus sistemas de TI. Así también se debe conocer en que medida la entidad recurre a la subcontratación para cumplir con sus objetivos y cuán completo el proceso de negocio ha sido trazado en un entorno de TI[15]. El auditor debe utilizar esta información para identificar problemas potenciales, formulando los objetivos y el alcance del trabajo, realizando el trabajo y teniendo en cuenta las medidas de gestión para las cuales los auditores de TI deben estar alerta.

12.4 De acuerdo con el enfoque de auditoría basado en el riesgo, los riesgos de control estarán relacionados con estos elementos de los controles generales y controles de aplicación de TI. A mayor riesgo de control, mayor es la necesidad de realizar más pruebas sustantivas.

12.5 En general, los auditores de TI están llamados a probar los controles relacionados con la tecnología, mientras que otros auditores prueban los controles financieros, regulatorios y de cumplimiento. El papel del auditor es entender el negocio potencial y los riesgos de TI que enfrenta la entidad auditada y, a su vez evaluar si los controles utilizados son adecuados para cumplir el objetivo de control. En el caso de los controles generales de TI, es importante que el auditor entienda las categorías generales y el alcance de los controles generales en funcionamiento, evalúe la supervisión de la gestión y la sensibilización del personal de la entidad sobre este punto, y averigüe cuán eficaces son los controles en la prestación de la función prevista. Incluso en pequeñas entidades en las que los sistemas de información y procesos de negocio relevantes para la presentación de informes financieros son menos sofisticados, su papel es significativo.[16] Si los controles generales son débiles, disminuyen considerablemente la fiabilidad de los controles asociados con las aplicaciones de TI individuales. Será importante para los auditores de TI entender la función asignada a la aplicación de TI con el flujo de trabajo asociado. Los auditores de TI deben ser capaces de identificar cada entrada, los procesos llevados a cabo por dicha aplicación y los resultados generados de ésta. La comprensión de los datos maestros que influyen en la entrada, el proceso y los productos y su seguridad, ayudará a los auditores de TI a evaluar la conformidad del sistema de TI con los requisitos de exactitud, integridad, completitud, confidencialidad, disponibilidad, fiabilidad, pertinencia y cumplimiento de los datos, a lo largo de las etapas de procesamiento de la información, captura y procesamiento de datos y la entrega/ salida de información.

[15] Las entidades que pasan de un entorno manual a uno computarizado, normalmente adoptarían un ejercicio de reingeniería de procesos de negocio (BPR). Se podría observar que algunos de los procesos de negocio se siguen llevando a cabo de forma manual, junto con una interface con los sistemas de TI. Estos escenarios especiales presentarían áreas de interés específico para los auditores de TI.

[16] ISSAI 1315 Identificación y evaluación de los riesgos de irregularidades importantes a través de una comprensión de la entidad y su entorno.

12.6 Sobre la base de la comprensión desarrollada del sistema de información y la entidad auditada, el auditor de TI puede decidir sobre su enfoque para las auditorías de TI. La auditoría de TI incluiría, eventualmente, la auditoría de la gobernanza de TI, los controles generales de TI y los controles de aplicación de TI o una combinación de éstos.

13. Selección de la muestra apropiada de auditoría de TI

Una muestra de auditoría[17] es la aplicación de los procedimientos de auditoría a menos del 100 por ciento de los elementos dentro de un grupo o población de relevancia de auditoría, de tal manera que todas las unidades de muestreo tienen una oportunidad de selección, a fin de proporcionar al auditor una base razonable para sacar conclusiones sobre toda la población. Esto también es aplicable a la selección de una muestra para la auditoría de TI. Por otra parte, cuando se diseña una muestra de auditoría, el auditor de TI deberá considerar el propósito del procedimiento de auditoría, las características de la población de la que se extrajo la muestra y las técnicas y herramientas utilizadas para extraer la muestra y analizarlas.

El auditor de TI debe determinar un tamaño de muestra suficiente para reducir el riesgo de muestreo a un nivel aceptablemente bajo. El auditor de TI deberá seleccionar los elementos de la muestra de tal manera que, cada unidad de muestreo en la población tenga una oportunidad de ser seleccionada. Auditar en un entorno TIC puede facilitar el análisis del 100 por ciento de la población, sobre todo en la fase de evaluación preliminar ***(Sección 21, a continuación)***. Sin embargo, para la realización de cualquier prueba sustantiva ***(Sección 21, a continuación)*** o exámenes detallados, aún se podría requerir extraer una muestra. Los auditores de TI pueden utilizar las directrices de la ISSAI 1530 u otros procesos derivados en uso en su EFS para la selección de la muestra.[18]

14. Objetivos de la auditoría de TI

Requisito:

Los objetivos de la auditoría de TI deben ajustarse a las áreas de riesgo identificadas durante la planificación de auditoría de TI a nivel de equipo, dependiendo del tipo de enfoque de auditoría que se contempla - auditoría financiera, de cumplimiento o de desempeño.

Explicación:

14.1 Los objetivos de la auditoría de TI consistirán en examinar si los procesos y recursos de TI en conjunto, logran alcanzar los objetivos previstos por la organización para asegurar la eficacia, eficiencia y economía en sus operaciones, cumpliendo con las normas existentes y equilibrando los riesgos al mismo tiempo.

14.2 De este modo, las auditorías de TI podrían ser auditorías de un sistema de TI total o de asuntos específicos, como son la seguridad de TI, la adquisición de la solución de negocio, los controles generales de TI, los controles de aplicación, el desarrollo de sistemas y la continuidad del negocio, u otras áreas que se mencionan en el Manual WGITA IDI.

14.3 La auditoría de TI atraviesa transversalmente los dominios de la auditoría financiera, la auditoría de cumplimiento o la auditoría de desempeño. Las auditorías de TI pueden ayudar a los tres tipos de auditorías o pueden llevarse a cabo en el contexto de cualquiera de ellas o una combinación de ellas.[19]

14.4 Objetivos con respecto a las auditorías financieras

[17] ISSAI 1530, Auditoría Financiera, Muestreo de Auditoría.

[18] ISSAI 1530, Directriz de Auditoría Financiera, Muestreo de Auditoría, Página 15.

[19] ISSAI 100 - "Las EFS también podrán efectuar auditorías combinadas, incorporando aspectos financieros, de desempeño y/o de cumplimiento.".

La definición de la auditoría financiera[20] describe las cuestiones relativas a la confianza, la preparación de los estados financieros de conformidad con un marco de presentación de informes financieros y la presentación de los estados financieros, conformándose de manera justa a los requisitos de importancia relativa. Esto cubre los objetivos generales relativos a la garantía del sistema financiero de cumplir con el marco de presentación de informes en la preparación de los estados financieros y la presentación de los informes de resultados financieros sin errores significativos. Es necesario, por lo tanto, que un sistema de TI mapee todos los requisitos para la preparación de los estados financieros, es decir, la captura de la información financiera, la aplicación de los requisitos del marco, el procesamiento de la información, y la presentación en el formato requerido. En términos generales, se trata de cuestiones relacionadas con la aplicación de controles de entrada, procesamiento y salida, además de los datos maestros y la seguridad de la aplicación. Sin embargo, los controles de aplicación son dependientes del apoyo adecuado de los controles generales de TI y la gobernanza de TI. Por lo tanto, los auditores financieros deberían poder obtener una seguridad de la idoneidad del sistema de TI y sus controles asociados, antes de concluir su auditoría. La seguridad en el sistema de TI debería ser obtenida a través de una auditoría de TI del sistema que analice todos los aspectos de la gobernanza de TI, los controles generales de TI y los controles de aplicación de TI.

Habiendo seguridad como resultado de una auditoría de TI plenamente desarrollada, puede que no sea esencial llevar a cabo una auditoría de TI durante cada auditoría financiera del mismo sistema, si hay una garantía de que ningún cambio y ningún daño del sistema ha sucedido durante el período desde la última auditoría de TI.

14.5 Objetivos con respecto a las auditorías de cumplimiento

La auditoría de cumplimiento es la evaluación independiente de si una materia determinada está conforme con las normas y regulaciones aplicables identificadas como criterios. Las auditorías de cumplimiento se llevan a cabo mediante la evaluación de si las actividades, operaciones financieras e información cumplen, en todos sus aspectos significativos, con las autoridades que rigen a la entidad auditada.

El objetivo de la auditoría de cumplimiento del sector público es permitir a la EFS evaluar si las actividades de las entidades del sector público cumplen con las normas y regulaciones que rigen estas entidades. Esto involucra presentar informes sobre el grado en que la entidad auditada cumple con los criterios establecidos. La auditoría de TI permite que se efectúe esta determinación para los sistemas automatizados. La auditoría de cumplimiento puede tratar sobre la regularidad (cumplimiento con los criterios formales, tales como leyes, regulaciones y convenios relevantes) o sobre la idoneidad (observancia de los principios generales que rigen una sana administración financiera y el comportamiento de los funcionarios públicos). Mientras que la regularidad es el enfoque principal de la auditoría de cumplimiento, la idoneidad puede ser un asunto pertinente dado el contexto del sector público, en el que existen ciertas expectativas relacionadas con la administración financiera y el comportamiento de los funcionarios públicos y de las entidades del sector público. Dependiendo del mandato de la EFS, el alcance de la auditoría puede, por lo tanto, incluir aspectos sobre idoneidad[21].

Los objetivos y características de la auditoría de cumplimiento describen la necesidad de cumplir con el debido proceso, la regularidad y la idoneidad. También se requiere que el sistema de TI en una entidad del sector público cumpla con las leyes y reglamentos aplicables, así como las normas y directrices adoptadas por la entidad. Los auditores de TI deben evaluar el cumplimiento por parte del sistema de TI de dichos reglamentos, así como las normas, directrices y diferentes parámetros de desempeño de la entidad para obtener una conclusión de auditoría. Toda esta evaluación se llevará a cabo basada en los criterios identificados derivados de las reglas, leyes, normas, criterios de

[20] ISSAI 200 - Principios Fundamentales de la Auditoría Financiera.
[21] ISSAI 400 - Principios Fundamentales de la Auditoría de Cumplimiento.

desempeño o incluso los requisitos de idoneidad. La evaluación del cumplimiento en relación a la gobernanza de TI, implicará garantías sobre los mecanismos para asegurar que las funciones de gobernanza se estén llevando a cabo y monitoreando periódicamente, que el mecanismo de control interno esté funcionando eficazmente y que todas las políticas de TI se estén aplicando conforme a lo previsto. La evaluación del cumplimiento en relación a los controles generales de TI implicará la evaluación de la existencia de controles con mecanismos de control y mitigación de riesgos adecuados implementados y la adhesión a las normas prescritas y parámetros de desempeño en la entidad. La evaluación de los controles de aplicación de TI, implicará la evaluación de la existencia de mapeo de procesos de negocio y reglas en el sistema de TI, y controles de entrada, proceso y salida relacionados con la validación de datos, integridad, exactitud y fiabilidad de los procesos.

La auditoría de cumplimiento por parte de un sistema de TI puede, invariablemente, requerir el uso de Técnicas de Auditoría Asistidas por Computador (CAAT) para llevar a cabo el análisis de la información e identificar excepciones.

14.6 Objetivos con respecto a las auditorías de desempeño

La auditoría de desempeño es una revisión independiente, objetiva y fiable sobre si los proyectos, sistemas, operaciones, programas, actividades u entidades gubernamentales están operando de acuerdo con los principios de economía, eficiencia y eficacia y si hay margen de mejora.

Los auditores de TI examinarán los sistemas de TI implementados con respecto a los criterios de economía, eficiencia, eficacia y valor para el ciudadano.

El examen de la economía en relación con la implementación de sistemas de TI sería destinado esencialmente a la minimización de los costos de los recursos a lo largo del ciclo de vida del sistema de TI, es decir, desde la adquisición del sistema para la implementación del mismo y su funcionamiento regular. En caso de la externalización de las funciones, el costo de dicha externalización debe ser minimizado. Una de las mejores maneras de minimizar estos costos es a través de un análisis del mercado. Sin embargo, la definición ineficiente de requerimientos de usuario debido a un conocimiento inadecuado de los requisitos por parte de la entidad, puede obstaculizar tal enfoque y dar lugar a mayores costos. La evaluación de la posibilidad de que los servicios de TI externalizados podrían haber sido llevados a cabo con los recursos disponibles, indicará un uso ineficiente de los recursos. Por lo tanto, durante la auditoría de desempeño de adquisiciones de TI, los auditores de TI podrían poner énfasis en las limitaciones de la entidad o el proceso de adquisición, según sea el caso.

El examen de la eficiencia en relación a la implementación de los sistemas de TI implicaría aumentar al máximo la utilización de los recursos o reducir al mínimo su utilización ineficiente, manteniendo la cantidad (integridad), la calidad (exactitud y fiabilidad) y el tiempo (disponibilidad) de la producción. Los auditores de TI pueden señalar las ineficiencias si hay duplicación de los procesos, demora indebida de cualquier proceso, controles innecesarios incorporados en el sistema, etc.

El examen de la eficacia en relación a la implementación de los sistemas de TI, implicaría establecer si ha cumplido sus objetivos, lo que entre otras cosas, implica cumplir con las metas y objetivos generales de la entidad. La no consecución de los objetivos de la entidad mediante la utilización del sistema de TI podría indicar la utilización ineficaz del mismo.

La auditoría de desempeño también contribuye a la rendición de cuentas y la transparencia. Ella se centra en las áreas en las que puede aportar un valor añadido para los ciudadanos y que tienen el mayor potencial de mejora. Además, proporciona incentivos constructivos para los responsables de tomar las medidas apropiadas. La implementación de TI, en la mayoría de los gobiernos y sus organizaciones, es a menudo una iniciativa novedosa. Consecuentemente, para que el enfoque de la auditoría de desempeño en la auditoría de TI promueva la gobernanza, el uso de los sistemas de TI de manera constructiva debe ser una de las piedras angulares del enfoque de los auditores de TI. Las

deficiencias descubiertas deben señalarse de una manera que conduzca a mejoras en el sistema, en lugar de matar la iniciativa.

14.7 Los auditores de TI pueden ser llamados a prestar asistencia en las auditorías en uso de CAATs. Las condiciones del encargo, en tal caso, serán útiles para decidir si la intervención constituiría una auditoría de TI. El uso de CAAT sólo para llevar a cabo el análisis de datos no es una auditoría de TI donde no se lleva a cabo la evaluación de un sistema TI.

15. Alcance de la auditoría de TI

Requisito:

Los auditores de TI deben determinar el alcance de la auditoría durante la etapa de planificación para asegurar el logro de los objetivos de la auditoría.

Explicación:

15.1 Una vez decididos los objetivos de las auditorías de TI, los auditores de TI también deben decidir acerca del alcance de la auditoría. Generalmente, los dos pasos se realizan de forma simultánea. El alcance de la auditoría de TI implicará decidir la extensión del examen de auditoría, en función de la cobertura de los sistemas de TI y sus funcionalidades, los procesos de TI a auditar, la ubicación de los sistemas de TI a cubrir, el período de tiempo a cubrir y, además, el tipo de auditoría (auditoría financiera / de cumplimiento / de desempeño). Será, básicamente, el establecimiento o la delimitación de los límites de la auditoría.

15.2 Los sistemas de TI apoyan las funciones de negocio en una entidad y por lo general implican procesos de TI específicos, como la introducción de datos en el sistema, la solicitud de información y la generación de informes. La mayoría de los sistemas de TI se encuentran en una ubicación especializada junto con el equipo de red asociado. La seguridad de la ubicación física y los equipos que contenga podría ser cubierta en la auditoría de TI.

15.3 El auditor debe seleccionar el período de tiempo para el análisis de auditoría (es decir, abordar la información de 1 año, 3 años, o más, etc.) que le permita a los auditores de TI sacar conclusiones adecuadas en las auditorías realizadas. Al auditar el sistema de TI, el período de tiempo a ser cubierto puede ser definido a partir de los requisitos de la auditoría correspondiente.

15.4 El alcance de la auditoría también implicará centrarse en dominios específicos del sistema de TI que serían de relevancia para el objetivo de la auditoría de TI. Los dominios de TI típicos son la gobernanza de TI, desarrollo y adquisición, operaciones de TI, contratación externa, seguridad de SI, plan de continuidad de negocio y plan de recuperación de desastres, y controles de aplicación[22]. Estos dominios serían generalmente suficientes para cualquier sistema de TI. Sin embargo, como el campo de TI está en constante cambio, los auditores de TI no deben excluir las posibilidades de nuevas áreas a ser sometidas dentro del alcance de sus auditorías, si se consideran pertinentes[23]. Una auditoría de TI integral requeriría el examen de todos los dominios de TI.

15.5 El alcance de la auditoría depende del perfil de riesgo del sistema de TI que está siendo auditado, así como de los recursos disponibles. Si los riesgos son mayores, el alcance puede que tenga que ser estrecho, pero extenso en la cobertura dentro del alcance de la auditoría de TI.

16. Capacidades de una EFS para llevar a cabo las auditorías de TI

Requisito:

La EFS deberá tener la capacidad adecuada para llevar a cabo la auditoría de TI.

---

[22] Manual WGITA-IDI sobre auditorías de TI para Entidades Fiscalizadoras Superiores.

[23] Capítulo 9, temas de interés adicionales, WGITA-IDI Manual sobre Auditorías de Tecnologías de la Información para las Entidades Fiscalizadoras Superiores.

La EFS deberá desarrollar la capacidad adecuada, si esta no está disponible, antes de comenzar una auditoría de TI.

Explicación:

16.1 La función básica de todas las EFS es auditar y puede que ya posean las capacidades de auditoría. Sin embargo, la auditoría de TI requiere capacidades específicas. Algunas de las capacidades que un equipo de auditoría de TI debe poseer colectivamente son:

i. Personal con experiencia y habilidad en TI;

ii. Comprensión de las reglas y reglamentos existentes o del entorno, en el que el sistema de TI está funcionando;

iii. Comprensión de las normas/directrices de auditoría de TI aplicables a la EFS;

iv. Comprensión de las técnicas de TI para recoger la evidencia de auditoría de sistemas automatizados;

v. Comprensión de las herramientas de auditoría de TI adecuadas para recoger, analizar, reproducir los resultados de dicho análisis o volver a realizar las funciones auditadas;

vi. Adecuada infraestructura de TI para capturar y retener la evidencia de auditoría;

vii. Disponibilidad de instrumentos de auditoría adecuados para analizar los datos recogidos.

17. Asignación de recursos

Requisito:

La EFS deberá identificar y asignar recursos suficientes y competentes para llevar a cabo la auditoría de TI.

Explicación:

17.1 Las EFS tienen muchas opciones diferentes para asignar recursos a la auditoría de TI.

17.2 El enfoque más común es tener un grupo central con especialistas en TI o expertos que ayudan a otros en el organismo a llevar a cabo las auditorías de TI. La EFS debe ser capaz de aprovechar las habilidades de unos pocos para llevar a cabo las auditorías de TI, en caso que estén recién empezando por este camino.

17.3 Otra opción es colocar especialistas de TI en cada uno de los equipos dentro de la EFS. Sin embargo, si cada equipo lleva a cabo sólo unas pocas auditorías de TI, entonces esto podría ser un uso ineficiente del especialista en TI. A medida que el número de auditorías de TI aumenta, las EFS tienden a establecer una función o grupo de auditoría de TI especializado. Este grupo es, entonces, el responsable de llevar a cabo todas las auditorías de TI que la EFS realiza.

17.4 El grupo de TI puede interactuar con otros equipos en la EFS que tengan un acervo de conocimiento de la entidad, esto permite que el equipo de auditoría de TI obtenga rápidamente una comprensión de la misión de la entidad y relacione sus procesos de negocio para apoyar el sistema de TI a fin de facilitar la auditoría de TI.

18. Contratación de recursos externos

Requisito:

La EFS puede considerar la participación de recursos externos para llevar a cabo la auditoría de TI, si la capacidad no está disponible.

Explicación:

18.1 La EFS puede decidir utilizar recursos externos para llevar a cabo la auditoría de TI o externalizar la auditoría de TI a un equipo externo, si tiene recursos limitados. Tales recursos serán principalmente consultores o contratistas externos que sean expertos en técnicas y herramientas de auditoría de TI, incluyendo bases de datos, programación y otras áreas relevantes para la auditoría de TI. Los recursos también incluyen cualquier infraestructura de TI necesaria en la EFS para realizar la auditoría. Por lo general, son los mismos que se utilizan para llevar a cabo cualquier otra auditoría, sin embargo, la auditoría de TI podría requerir un análisis específico, conversión de datos y el uso de herramientas de almacenamiento.

18.2 El trabajo de los recursos externos, cuando se han externalizado recursos, debe ser controlado adecuadamente por la EFS, a través de un contrato documentado o un acuerdo de nivel de servicio. El trabajo y los productos finales entregados a la EFS deben seguir los procesos y normas existentes adoptadas por la EFS. Esto significa que la EFS en cualquier caso requerirá de personal interno calificado e informado para supervisar el trabajo.

19. Vinculación con la entidad auditada

Requisito:

La EFS deberá vincularse con la entidad auditada antes del inicio de la auditoría.

Explicación:

19.1 Como en cualquier auditoría la entidad auditada deberá estar familiarizada con el alcance, los objetivos y los criterios de evaluación de la auditoría, los que deben ser discutidos con ella cuando sea necesario. La EFS puede, si fuere necesario, escribir la carta de compromiso a la entidad auditada, donde también podrá establecer los términos de dichos compromisos.

19.2 En concreto para la auditoría de TI, la EFS debe asegurarse de que se busque la debida cooperación y el apoyo de la entidad auditada en la realización de la auditoría, incluyendo tanto el acceso a los registros y la información, como las disposiciones adoptadas para obtener los datos electrónicos en el formato necesario para permitir el análisis.

20. Evidencia de auditoría

Requisito:

La EFS se asegurará de que las evidencias de auditoría sean suficientes, fiables y precisas para sostener las observaciones de la auditoría.

Las evidencias de auditoría estarán disponibles para recrear y revisar el proceso de auditoría posterior al cierre de la auditoría.

Explicación:

20.1 La evidencia de auditoría es la recopilación de datos, registros, documentos e información obtenida por los auditores de TI para fundamentar sus observaciones a la parte interesada(s) correspondiente, en el período en cuestión (en el momento de la auditoría o posteriormente), de manera suficiente, fiable y exacta.

20.2 Como tal, la evidencia debe tener las características de suficiencia, fiabilidad y exactitud/precisión de acuerdo con las normas de garantía de calidad internas de la EFS.

20.3 La evidencia en una auditoría de TI debe ser adecuadamente recogida y almacenada de forma que esté disponible en el futuro sin que los datos sean alterados. Los auditores de TI

necesitan asegurarse de que la evidencia tenga registro de fechas[24] para el caso que se realicen cambios, para evitar que la evidencia pueda ser alterada.

20.4 Las auditorías de TI presentan diferentes y específicas maneras de identificar, recoger, almacenar y retener evidencia. La evidencia podría recogerse de las pruebas específicas realizadas sobre las muestras bajo observación de auditoría. Los auditores de TI podrían llevar a cabo las pruebas en todas las operaciones o en una muestra, según sea necesario, pero los datos electrónicos siempre se pueden probar en su totalidad. Sin embargo, la prueba de las excepciones, en su caso, puede llevarse a cabo de forma selectiva, si las hay en gran número. La muestra de auditoría puede ser elegida al azar o de manera sistemática. Pueden utilizarse muestreos de unidades monetarias o también es posible que la muestra sea seleccionada con base a una decisión razonada de los auditores de TI.

20.5 Las técnicas y herramientas específicas para recolectar evidencia de auditoría en las auditorías de TI se discuten a continuación en la sección D.

21. Ejecución de la auditoría – Recopilación de evidencia de auditoría

Requisito:

El auditor de TI debe reunir evidencia de auditoría adecuada y suficiente, y analizar la misma para asegurar que los objetivos de la auditoría sean abordados adecuadamente.

Explicación:

21.1 Evaluación preliminar de los controles de TI

Los auditores de TI deben llevar a cabo una evaluación preliminar de los controles de TI en el sistema objeto de la auditoría, para obtener la seguridad de que los controles de TI existentes (controles de TI generales y controles de aplicación) son fiables y funcionan bajo un marco de gobernanza de TI adecuado. La evaluación de los controles a este nivel incluiría:

a) Evaluar que los mecanismos adecuados de gobernanza de TI estén establecidos y funcionando;

b) Evaluar que los objetivos de TI estén alineados con los objetivos de negocio;

c) Evaluar que los mecanismos adecuados estén establecidos para:

   i. La gestión efectiva de proyectos de TI ;

   ii. La adquisición y desarrollo de una solución de TI (que abarca aplicaciones de TI, hardware, software, personal, red, soluciones de servicios, etc.);

   iii. El funcionamiento de los sistemas de TI;

   iv. Asegurar la seguridad de la información;

   v. Garantizar la continuidad del negocio y la recuperación de desastres;

   vi. Garantizar una adecuada gestión del cambio;

   vii. Garantizar la entrega del servicio y retroalimentación;

   viii. Asegurar el cumplimiento de normas, reglamentos y procedimientos establecidos a través de monitoreo y control.

Los anteriores, salvo el punto (vii), comprenden controles generales de TI que no son específicos para cualquier flujo de operación individual o aplicación, sino que se relacionan con la

[24] Un sello de tiempo es un dato que se añade a la información (electrónica, papel, vídeo, etc.) para etiquetar el momento en que se generó, recopiló o editó la información. Las sellos de tiempo pueden ser tan detallados como sea necesario (día, fecha, horas, minutos, segundos, milisegundos, etc.) para la información.

infraestructura global de TI de la entidad, incluyendo las políticas, procedimientos y prácticas de trabajo relacionadas con TI, así como los controles de las operaciones del centro de datos (políticas y normas de TI), adquisición y mantenimiento del sistema de software, seguridad de acceso (físico y lógico), separación de funciones, continuidad de negocio y controles de recuperación de desastres, y desarrollo y mantenimiento de sistemas de aplicación.

Complementando la evaluación de los controles generales de TI cabría considerar la comprensión de los procesos de negocio, el mapeo de los procesos de negocio en el sistema de TI y los controles de aplicación de TI asociados.

Las excepciones identificadas después de una evaluación preliminar, conducirían a las decisiones sobre las pruebas sustantivas del sistema de TI y sus controles.

21.2 Prueba sustantiva

Las pruebas sustantivas consideran pruebas detalladas de los controles de TI, como en la evaluación preliminar, empleando diversas técnicas y herramientas para la investigación, extracción y análisis de datos. En la prueba sustantiva, las pruebas están diseñadas para corroborar las afirmaciones de acuerdo con los objetivos de auditoría. Las pruebas tienen que ser diseñadas específicamente, utilizando una o más de las técnicas[25] descritas en la sección D.

22. Supervisión y revisión

Requisito:

La EFS deberá garantizar que las auditorías de TI sean supervisadas y revisadas periódicamente.

Explicación:

22.1 El trabajo del personal de auditoría debe ser adecuadamente supervisado durante la auditoría y el trabajo documentado debe ser revisado por el líder del equipo de auditoría de TI (Elemento 5 - Desempeño de auditorías y otros trabajos' - ISSAI 40). El miembro senior del equipo debe tener la competencia necesaria para proporcionar orientación y asumir el rol de mentor y guía durante la realización de la auditoría.

23. Casos de fraude, corrupción y otras irregularidades

Requisito:

Las EFS y los auditores de TI deben identificar y evaluar los riesgos y fraudes pertinentes a los objetivos de las auditorías de TI.

La EFS deberá tomar las acciones que correspondan, según lo establecido en la ley pertinente, para tratar los casos de fraude, corrupción y otras irregularidades.

Explicación:

23.1 En la realización de la auditoría, los auditores de TI pueden encontrarse con casos de fraude, corrupción e irregularidades asociadas. Los requisitos para formular una denuncia de fraude pueden estar contenidas en el mandato de auditoría o en normas generales, como leyes o reglamentos, y puede ser necesario que el auditor comunique estas cuestiones a terceros ajenos a la entidad auditada, tales como las autoridades regulatorias u otras competentes. En tal situación, la EFS debe tomar las medidas que fueren procedentes, en los términos definidos por la norma aplicable.

23.2 En la realización de la auditoría, los auditores de TI deben mantener una actitud de escepticismo profesional y estar alertas a la posibilidad de fraude en todo el proceso de auditoría.

[25] Las técnicas pueden ser utilizadas en las pruebas de cumplimiento y sustantivas. El auditor de TI puede elegir una o más de estas técnicas, mientras realiza cualquiera de las dos evaluaciones.

24. Limitaciones

Requisito:

La EFS debe identificar, hacer presente y comunicar las limitaciones a los niveles apropiados en todas las etapas de la auditoría.

Explicación:

24.1 Las limitaciones a la auditoría de TI deben ser representadas en cada etapa de auditoría de TI a los niveles apropiados, a través de una comunicación documentada y adecuada.

24.2 Las limitaciones a la auditoría de TI deben señalarse en el informe.

24.3 Las limitaciones típicas dicen relación con un acceso inadecuado a los datos e información, la falta de documentación adecuada del proceso de informatización, lo que lleva a los auditores de TI a idear sus propios métodos de investigación y análisis para obtener las conclusiones. Cualquier otra limitación que enfrenten los auditores de TI, debe señalarse adecuadamente en el informe.

25. Seguimiento

Requisito:

La EFS debe dar seguimiento a las observaciones o asuntos informados, que la auditoría de TI destaque como importantes.

Explicación:

25.1 Las EFS tienen un papel en el seguimiento de las acciones tomadas por el auditado, en respuesta a las cuestiones planteadas en un informe de auditoría. El seguimiento se centra en si la entidad auditada ha abordado adecuadamente las cuestiones planteadas, incluida cualquier implicación más amplia. Por ejemplo, si el mismo sistema de TI es utilizado por muchas organizaciones gubernamentales, una acción insuficiente o insatisfactoria por parte de la entidad auditada puede requerir un nuevo informe de la EFS.

D. TÉCNICAS Y HERRAMIENTAS DE AUDITORÍA DE TI

Requisito:

La EFS deberá implementar técnicas de auditoría de TI adecuadas, de conformidad con la naturaleza del trabajo de auditoría y los requisitos de los objetivos de la auditoría.

Explicación:

26. Identificación de las técnicas específicas de auditoría de TI

26.1 Las técnicas de auditoría de TI se relacionan con la implementación de métodos y procedimientos mediante los cuales se puedea estudiar el ambiente de control en un sistema de TI, se puede recoger la evidencia y hacer el análisis necesario para obtener seguridad sobre la idoneidad de los controles.

27. Técnicas de planificación

27.1 Durante la planificación de una auditoría a un sistema de TI, el auditor tiene que entender primero cómo una aplicación en particular apoya un proceso de negocio de la entidad auditada. Para este propósito, se necesita obtener información básica sobre la forma en que la funcionalidad de negocio fluye a través del sistema. Las técnicas de auditoría tradicionales como el estudio de documentos, las entrevistas con el personal clave - tanto los propietarios de procesos de negocios, como las personas en la organización de TI - y la observación de los procedimientos, son útiles para obtener una buena comprensión de cómo el sistema apoya el negocio de la entidad. El estudio de las políticas y procedimientos de TI, los manuales de usuario de aplicación específica, la documentación sobre contratos de externalización de TI, los documentos de diseño funcionales, los manuales de

referencia técnicos suministrados por el vendedor y la lista de informes (estándares y personalizados), ayudan a la comprensión del entorno en el que opera el sistema y la identificación de los riesgos de negocio derivados de las fallas de control.

27.2 Durante las etapas de planificación anual y de equipo de las auditorías de TI, son abordadas las evaluaciones de riesgo de los sistemas de TI que están siendo desarrollados o están en uso en varias entidades auditadas. Estas pueden ser objetivamente llevadas a cabo mediante la aplicación de las técnicas que se describen en la sección de planificación de este documento estándar.

28. Técnicas de ejecución de auditoría

28.1 La elección de las técnicas a utilizar sería crucial en la realización de las pruebas de cumplimiento y sustantivas. Durante la prueba sustantiva, éstas deben estar diseñadas para corroborar las afirmaciones de acuerdo con los objetivos de auditoría. Las pruebas tienen que ser específicamente diseñadas, usando una o más de técnicas[26], tales como entrevista, cuestionario, observación, revisión guiada (*walk-through*), diagramas de flujo, captura y análisis de datos, verificación, re-cálculo, reprocesamiento, confirmación de terceras partes, etc.

28.2 Para una evaluación de la idoneidad de los controles generales de informática - que abarcan los dominios de gobernanza de TI, adquisición y desarrollo de sistemas, operaciones de TI, seguridad de la información y planificación de la continuidad del negocio - las técnicas utilizadas son similares a las usadas en otros tipos de auditoría.

28.3 Las técnicas de auditoría específicas para la auditoría de TI son utilizadas principalmente para la evaluación de los controles de la aplicación de TI. Durante la prueba de los controles de la aplicación, el auditor necesita:

I. Identificar los componentes importantes de la aplicación y el flujo de información a través del sistema, y obtener una comprensión detallada de la aplicación mediante la revisión de la documentación disponible y la entrevista del personal adecuado.

II. Entender los riesgos de control de la aplicación de TI y su impacto mediante la revisión de la criticidad de los procesos de negocio que el segmento de aplicación afecta.

III. Desarrollar una estrategia de prueba para identificar las fortalezas y debilidades del control y la evaluación del impacto de las últimas.

28.4 Para una mejor comprensión del sistema objeto de la auditoría, incluyendo sus puntos de control claves y el desarrollo de la estrategia de prueba a ser adoptada, es siempre útil examinar la documentación relacionada, tales como las especificaciones de diseño funcional, la documentación de gestión de cambio desde el primer uso o la última auditoría, manuales de usuario, manuales de referencia técnicos suministrados por el vendedor, etc.

28.5 La estrategia de prueba también dependerá de factores tales como activos en riesgo, el tiempo de existencia de la aplicación de apoyo al negocio, la calidad de los controles internos, la sensibilidad de las operaciones, los cambios significativos de procesos de negocio que resultan en cambios en la aplicación y los resultados de la auditorías anteriores, si los hay.

28.6 Para la evaluación de la segregación de funciones y la autorización de entrada, sería importante revisar las descripciones de trabajo, unirlas con los privilegios asignados en el sistema, revisar los procedimientos de autorización y confirmar la existencia de registro de acciones de las cuentas de usuario que tienen privilegios de administrador. Este registro de acciones requiere testearse para evidenciar el manejo de la gestión.

[26] Estas técnicas pueden ser utilizadas en las pruebas preliminares y sustantivas. Las aplicaciones de muchas de las técnicas están disponibles en el Manual WGITA IDI sobre Auditorías de TI para Entidades Fiscalizadoras Superiores

28.7 Las entidades auditadas tendrán su propia combinación de hardware, sistema operativo, sistemas de gestión de bases de datos, aplicaciones de software, software de red, etc. Los auditores de TI deben ser capaces de reunir información de estas fuentes para llevar a cabo el análisis requerido de la aplicación de TI. La comprensión del sistema de TI y base de datos de la organización, como también los procesos de negocio involucrados, su criticidad para la organización, los protocolos involucrados, etc., es un paso esencial para la extracción de datos. La prueba sustantiva de la idoneidad de los controles de aplicación implica:

a. Extraer datos de negocio relevantes de la entidad;

b. Transformar y cargar los datos en una herramienta;

c. Realizar un análisis de datos;

d. Validar los resultados de las pruebas;

e. Sacar conclusiones de auditoría.

Estos procedimientos se pueden llevar a cabo por los auditores de TI, con la ayuda de las técnicas descritas en el anexo A.

29. Elección de un adecuado sistema de preservación de información

29.1 Los auditores de TI deben garantizar la conservación de los resultados y de la evidencia de la auditoría para que ellos se ajusten a los requisitos de fiabilidad, integridad, suficiencia y exactitud. Asimismo, es importante para los auditores de TI asegurar que el proceso de auditoría también se conserve para permitir la verificación posterior de los procedimientos de análisis de auditoría. Esto implica técnicas de documentación adecuadas, las que se tratarán posteriormente.

29.2 Durante el requerimiento de datos, y en la medida de lo posible, se puede usar una carta de acompañamiento. Si esto no es posible, se deben generar documentos internos donde se anote la información importante, como la fecha en que fueron entregados los datos, de qué archivo se creó el volcado de datos y[27] si los datos fueron provistos desde el entorno de producción o de algún otro entorno, etc. La evidencia electrónica generada y utilizada para la presentación de informes de auditoría debe estar relacionada con dichos documentos.

29.3 Los auditores de TI deberían decidir sobre la conveniencia de la utilización de una o más de las técnicas anteriores y asegurarse por sí mismos de la integridad y utilidad de la técnica. El uso de cualquiera de las técnicas anteriores no debería afectar la integridad del sistema de aplicación de la y sus datos en la entidad auditada.

30. Herramientas de auditoría de TI

Requisito:

La EFS deberá utilizar herramientas de auditorías de TI apropiadas para la evaluación del riesgo en el proceso de auditoría, conjuntamente con la capacidad y los recursos disponibles en la EFS.

Explicación:

30.1 La auditoría de TI requiere un buen conocimiento acerca de los procesos y técnicas, junto con competencia en el uso de las herramientas de auditoría de TI, ya que estas auditorías, por su propia naturaleza, se ocupan de la información que se almacena y se procesa en forma electrónica, de modo que el trazado de la auditoría no es visible desde fuera.

30.2 **Las técnicas de auditoría asistidas por computador (CAAT)** son herramientas de TI que ayudan a un auditor en la realización de diversas pruebas automatizadas para evaluar un sistema de

[27]El volcado de datos se define como una gran cantidad de datos transferidos desde un sistema o ubicación a otra

TI o de datos. Éstos son muy útiles en aquellos casos en que un volumen importante de datos de una entidad auditada está disponible en formato electrónico. Las CAAT son útiles para la prueba de los controles y las pruebas sustantivas en la auditoría financiera, la auditoría de cumplimiento y la auditoría de desempeño. El uso de las CAAT y la extensión de su uso, está determinado por varios factores durante las etapas de planificación y ejecución de la auditoría.

30.3 Utilidad de las CAAT:

Las CAAT son muy útiles para llevar a cabo las actividades de auditoría de TI, tales como el análisis de registro de usuario, los reportes de las excepciones, la totalización, la comparación de archivos, la estratificación, el muestreo, las búsquedas de duplicados, la detección de brechas, la antigüedad, los cálculos de campos virtuales, etc. (estos se elaboran en la sección sobre técnicas de auditoría de TI). El uso de las CAAT otorga muchas ventajas en comparación con el examen manual. Algunas de estas son:

a) Las pruebas sustantivas y el análisis de grandes volúmenes de datos se puede hacer en un corto espacio de tiempo y con menos esfuerzo;

b) Las pruebas se pueden repetir fácilmente en diferentes archivos/datos;

c) Las pruebas flexibles y complejas se pueden hacer con un cambio en los parámetros;

d) Documentación automatizada de pruebas y resultados de auditoría;

e) Implementación más eficiente de los recursos de auditoría.

30.4 Elección de CAAT cuando se realiza una auditoría de TI: El uso de CAAT tiene costos asociados en términos de software bajo licencia, compatibilidad de hardware y la existencia de personal de auditoría calificado. Por lo tanto, algunos factores importantes que deben considerarse al decidir sobre el uso de CAAT en la auditoría de TI son los siguientes:

a) ¿Proporciona un valor adicional a la auditoría el uso de CAAT?

b) ¿Van a ser repetidas las pruebas en otras/futuras auditorías de la misma entidad auditada u otras entidades auditadas cuya naturaleza del negocio y operaciones sean similares?

c) ¿Se procesan las operaciones en línea y/o en tiempo real?

d) ¿El uso de otras técnicas de auditoría implicaría mayores costos y tiempo extra?

30.5 Algunos ejemplos destacados de CAAT son:

- Un software de auditoría de propósito general es desarrollado para satisfacer las necesidades específicas de los auditores y contiene las pruebas regulares que se llevan a cabo por auditores de TI como parte de la auditoría. Además incluyen funciones comunes como la extracción de datos, resumen, antigüedad, estratificación, búsqueda de duplicados, etc;
- El lenguaje de consulta estructurado (SQL) es un lenguaje no procedimental y se utiliza para definir y manipular datos en sistemas de gestión de bases de datos relacionales (RDBMS);
- Las hojas de cálculo son también CAATs útiles y se pueden utilizar para ejecutar consultas sencillas, como la extracción de datos que cumplen criterios predeterminados, clasificación, totalización, etc;
- Las herramientas de minería de datos ayudan a descubrir patrones en grandes conjuntos de datos, a extraer información con ellos y a transformarlos en una estructura comprensible para su uso a través de la visualización de datos.
- Softwares de auditoría específicos para el sector industrial se desarrollan con el objetivo de

proporcionar funcionalidades para atender las tareas de auditoría más comunes asociadas con industrias específicas, es decir, que capturan la lógica específica de la industria para crear consultas de auditoría, etc. Se encuentran en las industrias con procesos de negocio bien documentados y establecidos, tales como la banca, manufactura, petróleo y gas, transporte marítimo, etc.

- El software utilitario realiza funciones diseñadas para ayudar a analizar, configurar, optimizar o mantener la infraestructura de TIC. Los principales ejemplos de software utilitarios relacionados con la auditoría de TI son, entre otros, utilitarios para el control de revisiones, depuradores, analizadores de espacio en disco, administradores de archivos, utilitarios de red y perfiladores de sistemas
- Algunos sistemas bien desarrollados han incorporado módulos de auditoría (software de auditoría especializado) que generan informes estandarizados, como también personalizados. Estos vienen como funcionalidades integradas de aplicaciones de planificación de recursos empresariales (ERP). Además, hay softwares comerciales en el mercado que dan a los auditores de TI acceso de sólo lectura a datos de ERP a través de aplicaciones.

30.6 Con el fin de utilizar CAAT para auditar un área particular, el auditor debería planificar en detalle. Es importante entender y obtener información/detalles, entre otros, sobre las relaciones de tablas/archivos, diccionario/triggers (detonantes) de base de datos, esquema de datos, controles totales, tamaño/formato de datos y documentación del sistema, antes de comenzar una auditoría activada por CAAT.

E. PRESENTACIÓN DE INFORMES

Requisito:

Los informes de auditoría de TI deberán reflejar los hallazgos del proceso de auditoría de TI, en función de materialidad de tales hallazgos en relación a los objetivos de la auditoría.

El informe de auditoría de TI deberá ser integral, equilibrado, convincente, oportuno y fácil de leer.

Explicación:

31. Requisitos de presentación de informes de una auditoría de TI

31.1 Dado que la auditoría de TI puede estar en la naturaleza de una auditoría financiera, de desempeño, de cumplimiento o de una combinación de éstas, los requisitos de presentación de informes de una auditoría de TI provendrán, del mismo modo, de las ISSAI 100-400 y dependiendo de la naturaleza de la auditoría que se lleva a cabo, de las ISSAI 1700, 1705 y las ISSAI 1706 en el caso de la auditoría financiera y las respectivas ISSAI nivel 4 sobre auditoría de cumplimiento y auditoría de desempeño.

31.2 Algunas consideraciones que los auditores de TI deben tener en cuenta son limitar el uso de la jerga técnica, tener en cuenta la sensibilidad de la información que se presenta en el informe, por ejemplo, contraseñas, nombres de usuarios, ID e información personal.

32. Contenidos y formato del informe de auditoría de TI

32.1 El formato general de un informe de auditoría de TI incluye lo siguiente;

a. Los objetivos de la auditoría;

b. El alcance de la auditoría;

c. Las fechas aplicables a la cobertura de la auditoría;

d. Los criterios de la auditoría;

e. La metodología de la auditoría;

f. El resumen;

g. Los hallazgos de la auditoría;

h. Las conclusiones de la auditoría;

i. Las recomendaciones de la auditoría;

j. Cualquier causa(s) y riesgo(s) asociado, restricciones, reservas, limitaciones o preocupaciones que el auditor pueda tener en relación con la auditoría realizada por él/ella.

32.2 A pesar de la naturaleza técnica de una auditoría de TI, los auditores de TI deben asegurarse de que el informe sea totalmente comprensible por la alta dirección, la entidad auditada, las partes interesadas y el público en general.

32.3 Los auditores de TI podrán debatir el proyecto de informe con el gestor del sistema de TI auditado antes de la finalización y publicación e incluir su respuesta a los hallazgos, conclusiones y recomendaciones en el informe final, si correspondiere.

32.4 La unidad auditada podrá decidir aceptar el riesgo de no corregir una condición informada debido al costo, la complejidad de la acción correctiva u otras consideraciones. El informe de auditoría de TI debe mencionar este hecho a las autoridades responsables, de acuerdo con su marco desarrollado internamente.

32.5 En caso que los auditores de TI y la unidad auditada no estén de acuerdo sobre una recomendación de auditoría o comentario en particular, el informe de auditoría puede exponer ambas posiciones y las razones de su desacuerdo en un apéndice. Como alternativa, las opiniones de la unidad auditada pueden ser presentadas en el cuerpo del informe o en una carta de presentación.

32.6 Los auditores de TI pueden considerar el posible impacto negativo del informe una vez que se publiquen los informes de las EFS. Por lo tanto, si los auditores de TI encuentran problemas de seguridad en el sistema de TI y los han informado antes de que el sistema informático sea reparado, la vulnerabilidad del sistema de TI es expuesta al público antes de ser corregida. En tal escenario, las EFS pueden considerar opciones tales como la presentación de informes después de que el sistema de TI sea reparado, o no informar de la vulnerabilidad en detalle, para evitar el efecto adverso del informe.

32.7 El seguimiento de cualquier auditoría es la culminación de todo el proceso de auditoría de TI. Se lleva a cabo para asegurar que las deficiencias que se han identificado en el curso de una auditoría de TI, hayan sido posteriormente abordadas de manera satisfactoria. Por lo general, es el resultado de una evaluación de riesgos continua que es llevada a cabo por una EFS. Como parte del seguimiento de una auditoría de TI cuyo informe ha sido presentado, el auditor de TI vuelve a revisar una auditoría después de un lapso de tiempo razonable para asegurar que se hayan aplicado todas las recomendaciones.

Anexo A - Técnicas de análisis de datos

1. **Extracción de datos de negocio relevantes de la entidad:**

   Comprender la estructura de datos mediante la obtención y el estudio de los documentos de definición de datos de la entidad auditada. Si la entidad auditada concede acceso de sólo lectura al sistema, entonces los datos almacenados en las tablas pertinentes para el ejercicio de auditoría, pueden ser extraídos mediante la consulta de la base de datos si se poseen las habilidades. De lo contrario, se puede solicitar a la entidad que proporcione una copia de los datos de origen pertinentes. Los datos pueden ser recibidos en forma de un volcado de base de datos que contenga un registro de la estructura de la tabla y/o los datos de una base de datos, usualmente en forma de una lista de comandos SQL. Los auditores de TI podrían tener que crear un ambiente similar (versiones compatibles de las aplicaciones más comunes de bases de datos, sistemas operativos, hardware, etc.) al de la entidad auditada para importar/analizar los datos de la copia de los volcados de datos extraídos. En muchos casos, esto representa el aspecto más importante de las pruebas de control de aplicación, ya que la correcta extracción de datos sienta las bases para el éxito de los procesos posteriores. También puede ser necesario que los auditores de TI conviertan los datos de una forma a otra para facilitar una mejor lectura y análisis.

2. **Transformación y carga de datos:**

   Utilice el software de auditoría/herramientas de extracción, transformación y carga, para importar datos desde diversas plataformas de base de datos. Las herramientas de análisis de datos utilizadas más comúnmente (analizadas en la sección sobre herramientas) permiten la importación de datos desde múltiples bases de datos, al formato de hoja de cálculo original de las herramientas. Estas herramientas suelen utilizar un asistente de importación para ayudar en la importación (interpretación, conversión, formato) de datos para su posterior análisis. Es importante que el auditor realice algunos pre-formateos de los datos de origen para hacer el ejercicio de análisis más fácil. También, podrían utilizarse un software de auditoría generalizado o un software utilitario específico para evaluar el funcionamiento de varias utilidades de los sistemas de TI. El uso de cualquiera de estos o su combinación, dependerá de los objetivos de la auditoría y el alcance a cubrir en las auditorías de TI.

3. **Realización del análisis de datos**

   Los pasos principales en el análisis de los datos de negocio de la entidad auditada para obtener seguridad sobre la calidad de los controles de aplicación son comunes a cualquier forma de análisis de datos. Las consideraciones claves en el análisis de datos son las siguientes:

   - Identificar el propósito del análisis o proyecto;
   - Comprender la muestra(s) en estudio;
   - Entender los instrumentos que se utilizan para recopilar datos;
   - Ser consciente de los diseños y formatos de datos[28]; y
   - Establecer un un identificador único si se combina o fusiona, en caso de ser necesario.
   - Los auditores de TI necesitan planificar:
     - La declaración de preguntas de investigación / objetivos

[28] Este sería uno de los pasos más importantes antes de la realización del análisis de datos. El diseño significaría la comprensión de las diferentes bases de datos, tablas incorporadas, patrón de codificación utilizado y relaciones entre tabla y bases de datos. La comprensión de los diferentes modelos de base de datos será útil en este sentido.

- Los métodos utilizados para responder a las preguntas de investigación
    - Los criterios para la evaluación
    - La evidencia
    - El análisis
    - La conclusión

- Los procedimientos de reestructuración de archivo (creación de sintaxis, adición de nuevas variables, según sea necesario)
- Los procedimientos de limpieza de datos (p. ej. la eliminación de valores atípicos)

La mayoría de los análisis se pueden ejecutar directamente desde un archivo de datos de trabajo. Algunos análisis pueden requerir transformaciones de datos brutos, subconjuntos o datos de entrada específicos para cumplir con el software de estadística o las herramientas que el auditor puede utilizar.

4. Comprensión de la representación y tipos de datos

El análisis de datos se realiza generalmente en una copia de los datos recibidos de la entidad auditada para preservar el original para su posterior confirmación y revisión, si fuese necesario.

Se puede utilizar un software de auditoría de propósito general o un software de auditoría especializado para llevar a cabo el análisis de la información. Estas herramientas ofrecen la facilidad de importar y analizar los datos. También se puede hacer uso de Lenguaje de Consulta Estructurado en el análisis de datos. Para sistemas complejos, como los sistemas ERP, la información está disponible a través de informes especificados. Los auditores de TI deben entender dichos informes y obtener informes pertinentes para llevar a cabo un análisis apropiado. Los auditores de TI deben tener cuidado en asegurar que los datos obtenidos sean fiables, competentes, razonables y suficientes. Deben ser, en la medida de lo posible, timbrados y debidamente examinados por la organización auditada.

En particular, las variables en varios campos de datos pueden requerir codificación especial para la representación diferente de datos

- Numérica
- *Cadena de caracteres*
- Fecha y hora
- Monetaria

Las técnicas individuales de análisis de datos para examinar la integridad de las aplicaciones son dependientes, nuevamente, de los objetivos de la auditoría. Estas técnicas son:

1. **Uso de datos de prueba:** El análisis con datos de prueba se hace en situaciones en las que se intenta probar la calidad del programa. La premisa es que es posible generalizar acerca de la fiabilidad general de un programa, si es fiable para un conjunto de pruebas específicas. El uso de los datos de prueba implica el *diseño* de datos de prueba y la *creación* de datos de prueba antes de ejecutar el programa con este tipo de datos. A menudo, esta técnica se implementa en la etapa de prueba de la aplicación por el propio desarrollador, antes de que una aplicación o cambios en ella sean trasladados a la producción (es decir, operación transaccional en curso). Mientras se audita un sistema de TI recientemente implementado, o procesos de gestión del cambio, el auditor puede revisar los procedimientos realizados en la fase de prueba.

2. **Comparación de código:** Los desarrolladores utilizan técnicas de comparación de código que implican la comparación del código fuente de un programa o de las modificaciones del mismo,

con metodologías de diseño estándar para el lenguaje de programación particular, con la intención de descubrir errores, fallas o brechas de seguridad de las convenciones de programación. En su mayoría son herramientas de los desarrolladores y no son utilizadas a menudo por los auditores de TI. Para las muestras de código seleccionadas por los equipos de pruebas de seguridad independientes, el papel de los auditores sería determinar que se ha probado la seguridad del código y que los resultados fueron documentados e informados, y que las violaciones y las vulnerabilidades detectadas fueron debidamente saneadas. Sin embargo, los auditores con las habilidades adecuadas, pueden recurrir a la comparación de código en relación con la gestión del cambio o la puesta en marcha de un programa de aplicación, si el alcance lo permite.

3. **Prueba de la integridad de datos:** La prueba de integridad de datos es un conjunto de pruebas sustantivas que examinan la exactitud, integridad, consistencia y autorización de los datos disponibles en el sistema. Estas pruebas indicarán la debilidad en los controles de entrada o de procesamiento. Las pruebas de integridad de datos ayudan a identificar la solidez de la integridad relacional, mediante la revisión de las rutinas de validación que se incorporaron en la aplicación, durante el diseño de las limitaciones de las condiciones de entrada y las características de los datos, en la etapa de definición de tabla del diseño de base de datos.

Estas pruebas implican ciertas técnicas de análisis de datos que los auditores de TI pueden implementar con la ayuda de herramientas de análisis comunes o de software de auditoría generalizados.

1. **Muestreo:** Las técnicas de muestreo son útiles para obtener conclusiones adecuadas basadas en controles estadísticamente suficientes de datos limitados. Hay dos métodos principales de muestreo utilizados por los auditores de TI. Estos son el muestreo de atributos y el muestreo de variables. El muestreo de atributos se utiliza generalmente en situaciones de pruebas de cumplimiento y aborda la presencia o ausencia del atributo, proporcionando conclusiones que se expresan en tasas de incidencia. El muestreo de variables se aplica generalmente en situaciones de pruebas sustantivas y aborda las características de la población que varían, facilitando conclusiones relacionadas con las desviaciones de la norma.

Para las validaciones de la prueba y otros controles de entrada en un sistema que trata con una gran cantidad de datos, el auditor puede encontrar útil extraer una muestra aleatoria de registros de transacciones almacenados en la base de datos del sistema.

La mayoría de las aplicaciones de análisis de datos, incluyendo aplicaciones de hoja de cálculo y software de auditoría de propósito general proveen funciones fáciles para seleccionar un elemento particular de datos (campos/ columnas/ tupla) y las celdas de datos relacionados, y crean subconjuntos aleatorios de los datos elegidos, mediante el uso de algoritmos basados en semillas de número aleatorios, o fórmulas simples.

2. **Resumen y estratificación:** Estas dos técnicas ayudan a la elaboración de perfiles de datos antes de que se lleve a cabo cualquier prueba de los controles. El resumen de datos ayuda a totalizar las transacciones en términos de atributos definidos, esto ayuda al auditor a obtener una comprensión global de las transacciones. Por ejemplo, totalizar las cuentas por cobrar por tipos de cliente proporciona una información útil sobre los morosos de pago de alto valor. Una función muy útil disponible en la hoja de cálculo y en las herramientas de auditoría de propósito general es la tabla dinámica, ayudando en la generación de la información resumida desde una base de datos grande, en un lapso muy corto de tiempo.

La estratificación de los datos prepara una distribución de frecuencia de los datos en términos de ubicaciones o intervalos definidos. Le puede dar al auditor información importante acerca de la naturaleza de los datos y también puede ayudar a identificar las áreas en las que deben realizarse las pruebas detalladas.

3. **Consultas condicionales**: La técnica de extracción de datos basada en consultas condicionales es útil para llevar a cabo una serie de controles sobre la calidad de los controles de aplicación que incluyen pruebas de completitud, de integridad, de mapeo correcto de las reglas de negocio.

a. Prueba de los controles de entrada: Por ejemplo, en un sistema de TI que puede prestar soporte a un determinado programa de educación / bienestar financiado por el gobierno, es importante crear registros de beneficiarios permanentes en forma de tablas de datos maestros en la base de datos. Una prueba de los controles de entrada en este caso consiste en extraer una muestra de registros maestros almacenados en la tabla maestra y comprobar si la captura de datos para los atributos relacionados (identificadores únicos, nombres, direcciones, identificación de direcciones) tienen espacios en blanco, valores sin sentido, duplicados, etc. Evidencia de cualquiera de estos errores indicaría deficiencias en las descripciones de datos durante el diseño de la tabla.

b. Prueba de controles de procesamiento: Para las pruebas de los controles de procesamiento una prueba sustantiva específica puede ser la de averiguar si una regla de negocio en particular está mapeada correctamente en el sistema de TI que se utiliza para hacer el procesamiento de negocios. Por ejemplo, en un sistema utilizado por una entidad competente en asuntos tributarios, la prueba podría consistir en asegurar que las condiciones para la concesión de devolución de impuestos estén mapeadas en el sistema. En este caso, se podría hacer una extracción de registros del conjunto de datos de impuestos de la muestra con una condición que simula la regla de negocio de acuerdo a la ley. Cualquier resultado de este ejercicio de extracción que no esté conforme con la condición de negocio, puede indicar un control de procesamiento indebido o la falta de mapeo de la regla de negocio. Tal falta de mapeo lleva a errores repetidos, los que podrían dar lugar a un impacto significativo en las finanzas de la entidad.

Los auditores de TI necesitan tener un conocimiento de dominio detallado de las reglas de negocio de la entidad para diseñar consultas condicionales significativas, a fin de verificar si las reglas de negocio están correctamente mapeadas en la aplicación.

1. **Identificación de duplicados:** Una prueba común de la integridad de datos relacionales en una base de datos es examinar la existencia de duplicados, donde lo lógico es que éstos no se presentaran, en función de las reglas de negocio definidas de la entidad. Por ejemplo, en una base de datos de la seguridad social o impuestos, la identidad relevante se define como única de acuerdo a la ley. La evidencia de duplicados en este campo de datos, indicaría validaciones incorrectas respecto de las entradas de datos permanentes, dando lugar a un riesgo operativo o financiero para la entidad auditada. Las herramientas de análisis proporcionan una función simple para detectar claves duplicadas. Estas se pueden encontrar incluso en tablas transaccionales, que podrían aumentar el riesgo de duplicación de pagos.

Los auditores de TI necesitan evaluar la necesidad de tales pruebas, dependiendo del control de aplicación que se está probando dentro del proceso. Por ejemplo, si el auditor está revisando los controles financieros dentro de las aplicaciones de procesamiento de cuentas por pagar, las posibilidades de que el número de orden de compra generado por el sistema sea duplicado, serían bastante improbables. Sin embargo, si el auditor necesita hacer pruebas por controles de presentación de facturas duplicadas de proveedor (una entrada externa), que es una entrada no generada por el sistema, esta prueba puede ser utilizada.

2. **Análisis de brechas:** El objetivo del uso de esta técnica consiste en determinar la integridad y detectar si existen brechas en un campo de datos numérico que se espera que tenga una numeración secuencial. En MS Excel esta se encuentra a través de la clasificación de valores en serie en el campo de datos en cuestión, añadiendo un campo calculado en base a la lógica secuencial y luego filtrando por filas donde se producen excepciones. El software de auditoría general utiliza una función simple de detección de brechas, donde el campo en cuestión debe

ser definido para la identificación de las brechas. Para utilizar las funciones de duplicado o de detección de brechas, el auditor no requiere mucha experiencia en consulta.

3. **Trabajo con múltiples archivos:** La base de datos fuente a menudo contiene gran número de tablas maestras y de transacción para satisfacer la necesidad de la normalización de los datos. Al trabajar con conjuntos de datos importados, a menudo es útil añadir juntos campos particulares en una tabla de datos, con el uso de una clave de combinación (campo). GAS permite dicha unión de varios archivos con la ayuda de la función de “unión'. El uso de las funciones de combinación o consultas condicionales en tablas combinadas, ayuda al auditor a evaluar la integridad referencial entre las tablas de datos o incluso entre aplicaciones de negocios relacionados separadas, que son usadas por la entidad.

Por ejemplo, si una entidad registra posibles proveedores en un portal web y utiliza una aplicación de adquisición separada para elevar las órdenes de compra, las reglas de negocio deben requerir que la base de datos de proveedores esté vinculada a la base de datos de adquisiciones. Unir tablas de estas dos bases de datos separadas, por medio de la combinación de nombres de proveedores e ID de proveedores ayudaría a establecer la adecuación de la interface entre las dos aplicaciones de negocios relacionados.

Los auditores de TI tienen que aplicar una combinación de estas técnicas para obtener una seguridad razonable sobre los controles de aplicación.