GUID 5100

Orientación sobre auditoría de sistemas de información

Junio 2019

Las Guías INTOSAI (GUID) son emitidas por la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI) como parte del Marco INTOSAI de Pronunciamientos Profesionales. Para más información visite www.issai.org

INTOSAI



INTOSAI, 2019

ÍNDICE

1. Introducción 4

2. Objetivo de este GUID 6

3. Definiciones 7

4. Alcance 8

5. Planificación de auditoría de los Sistemas de Información 9

6. Realización de Auditoría de SI 15

7. Informes sobre Auditoría de SI 21

8. Hacer un seguimiento 23

1 INTRODUCCIÓN

1.1 GUID 5100 proporciona el marco general para realizar auditorías de Sistemas de Información dentro del IFPP. El GUID está destinado a proporcionar la base para el desarrollo de futuros GUID en la serie 5100-5109 sobre el área temática de la auditoría de Sistemas de Información, dentro de IFPP.

1.2 El marco establecido en este GUID es consistente con los Principios Fundamentales de Auditoría del Sector Público (SISAI 100), Principios Fundamentales de Auditoría Financiera (ISSAI 200), Principios de Auditoría de Desempeño (ISSAI 300) y Principios de Auditoría de Cumplimiento (ISSAI 400).

1.3 Las Entidades Fiscalizadoras Superiores (EFS) tienen el mandato de auditar a los gobiernos y sus entidades según sus respectivos mandatos de auditoría.[1] A través de sus actividades, las EFS tienen como objetivo promover la eficiencia, la rendición de cuentas, la efectividad y la transparencia de la administración pública[2].

1.4 Los gobiernos y otras entidades del sector público han estado adoptando innovaciones en Tecnología de la Información (TI) en sus sistemas de información, con el fin de mejorar la eficiencia y la eficacia en su funcionamiento y prestación de diversos servicios públicos. Esto se debe a que la TI ha permitido capturar, almacenar, procesar, recuperar y entregar información electrónicamente, lo que a su vez crea un alcance significativo para mejorar la precisión, confidencialidad y puntualidad de los sistemas de información. Además, el modo de prestación de servicios públicos está pasando rápidamente de lo físico a lo electrónico, lo que hace que los gobiernos tengan que funcionar como plataformas digitales que brindan servicios, así como infraestructura para otros sistemas de información basados en TI.

1 INTOSAI-P 1 La Declaración de Lima
2 Resolución de la Asamblea General de las Naciones Unidas A/66/209

1.5 Esta transición a sistemas de información computarizados y procesamiento electrónico por parte de entidades auditadas en el sector público ha provocado un cambio significativo en el entorno en el que trabajan las EFS. El gasto del sector público en TI está creciendo. También es necesario garantizar que las entidades del sector público hayan adoptado controles internos de TI para mantener la confidencialidad, integridad y disponibilidad de los datos. Por lo tanto, se hace imprescindible que las EFS desarrollen la capacidad adecuada para realizar un examen exhaustivo de los controles relacionados con los sistemas de información.

2 OBJETIVO DE ESTE GUID

2.1 Las ISSAI 100, 200, 300 y 400 establecen los preceptos básicos de la auditoría en relación con la Auditoría Financiera, Auditoría de Desempeño y Auditoría de Cumplimiento. Estas ISSAI se relacionan con los principios generales, procedimientos, estándares y expectativas de un auditor. Son igualmente aplicables a las auditorías de los sistemas de información también.

2.2 El objetivo de este GUID es proporcionar orientación a los auditores sobre cómo realizar auditorías de desempeño y/o cumplimiento relacionadas con el tema específico de los sistemas de información o donde la auditoría de los sistemas de información puede ser parte de un trabajo de auditoría más grande que puede ser financiero, de cumplimiento o una auditoría de desempeño

2.3 Los auditores pueden aplicar el contenido de este GUID a las etapas de Planificación, Realización, Informes y Seguimiento del proceso[3] de auditoría.

3 ISSAI 100

3 DEFINICIONES

3.1 Sistemas de información: Los sistemas de información se pueden definir como una combinación de actividades estratégicas, gerenciales y operativas involucradas en la recopilación, procesamiento, almacenamiento, distribución y uso de la información y sus tecnologías relacionadas. La complejidad de dicho sistema de información puede variar desde un simple libro en el que las entradas para el recibo y el pago de dinero se mantienen manualmente, hasta un sistema más complejo impulsado por TI, como un sistema de evaluación de impuestos, en el que todos los procesos: recopilación de datos (por ejemplo, las declaraciones de impuestos presentadas a través del portal web en línea), el almacenamiento en los servidores, el procesamiento de la evaluación (basado en la programación utilizando las reglas de impuestos) y la comunicación de la demanda de impuestos, reembolso y reconocimiento (en tiempo real o en intervalos prescritos) - están automatizados. La tecnología de la información comprende el hardware, el software, la comunicación y otras instalaciones utilizadas para ingresar, almacenar, procesar, transmitir y emitir datos en cualquier forma.

3.2 La auditoría de los sistemas de información puede definirse como el examen de los controles relacionados con los sistemas de información basados en TI, con el fin de identificar casos de desviación de los criterios, que a su vez se han identificado en función del tipo de auditoría, es decir, auditoría financiera, auditoría de cumplimiento o auditoría de rendimiento.

4 ALCANCE

4.1 Los auditores pueden usar este GUID para llevar a cabo auditorías de desempeño y/o cumplimiento en el tema específico de los sistemas de información, así como también cuando la auditoría de los sistemas de información sea parte de un trabajo de auditoría más grande que puede ser un proceso financiero, de cumplimiento y/o auditoría de desempeño.

4.2 Esta directriz proporciona más orientación sobre cómo podría abordarse cualquier auditoría de los Sistemas de Información mediante el uso de auditorías financieras/de rendimiento/cumplimiento y no contiene ningún otro requisito para realizar la auditoría.

5

PLANIFICACIÓN DE AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

5.1 Las EFS pueden adoptar una planificación de auditoría basada en el riesgo para las auditorías de SI, en línea con el proceso descrito en ISSAI 100, ISSAI 200 (Auditoría financiera), ISSAI 300 (Auditoría de desempeño) e ISSAI 400 (Auditoría de cumplimiento), dependiendo de los objetivos de compromiso de la auditoría.

5.2 El trabajo de Auditoría de SI estará determinado por el objetivo y el alcance de la auditoría. Los ejemplos podrían incluir:

1) Evaluar los controles generales relevantes[4] y los controles de aplicación[5] que tienen un impacto en la fiabilidad de los datos de los sistemas de información, que a su vez tienen un impacto en los estados financieros de la entidad auditada.

2) Asegurar el cumplimiento de los procesos de los sistemas de información con las leyes, políticas y estándares aplicables a la entidad auditada.

3) Garantizar que los recursos de TI permitan alcanzar los objetivos de la organización de manera eficiente y efectiva, y que los controles generales relevantes y los controles de la aplicación sean efectivos en la prevención, detección y corrección de casos de exceso, extravagancia e ineficiencia en el uso y gestión de los sistemas de información.

5.3 En función de la evaluación de riesgos, el alcance de una Auditoría de SI

4 Los controles generales son procedimientos manuales o automatizados que tienen como objetivo garantizar la confidencialidad, integridad y disponibilidad de la información en el entorno físico dentro del cual se desarrollan, mantienen y operan los sistemas de información.

5 Los controles de aplicación son procedimientos automatizados o manuales dependientes de TI dentro de un sistema de información que afecta el procesamiento de transacciones, y puede relacionarse con la validación de datos de entrada, procesamiento preciso de datos, entrega de datos de salida y controles relacionados con la integridad de los datos maestros.

puede extraerse de cualquiera o de todos los siguientes dominios[6] de la entidad auditada:

1) Política organizativa sobre TI[7]
2) Estructura de gobierno organizativo en materia de TI
3) Controles generales proporcionados en el área de negocios que se automatiza
4) Gestión de activos
5) Desarrollo, adquisición y mantenimiento de sistemas de información, incluido el mapeo de procesos comerciales y la lógica de programación asociada
6) Gestión de operaciones de TI
7) Gestión del entorno físico
8) Administración de recursos humanos
9) Gerencia de comunicaciones
10) Gestión de seguridad de la información[8]
11) Gestión de cumplimiento legal
12) Continuidad del negocio y gestión de recuperación ante desastres
13) Gestión de controles de aplicaciones

5.4 Las EFS pueden seleccionar el período de tiempo para el análisis de auditoría (por ejemplo, un año, tres años, etc.) para definir el alcance del trabajo de Auditoría de SI. Se puede seleccionar un período de tiempo apropiado, que sea relevante para los objetivos definidos para el trabajo de auditoría.

5.5 Cuando una Auditoría de SI es parte de un trabajo de auditoría, la EFS puede garantizar que el equipo de auditoría en su conjunto trabaje de manera integrada para lograr el objetivo general de auditoría. Para lograr una integración efectiva, las EFS pueden considerar:

1) Documentación exhaustiva del trabajo a realizar por los auditores de SI
2) Formulación de un protocolo para compartir información entre los auditores de SI y otros auditores;
3) Identificación de qué sistemas de información y objetivos de control están

6 La mayoría de los dominios descritos han sido adaptados de SIO/IEC 27001
7 Incluyendo aspectos de Gestión Estratégica
8 Incluyendo seguridad cibernética

dentro del alcance de la auditoría;

5.6 Las EFS pueden garantizar que el equipo de auditoría esté compuesto por miembros que colectivamente tengan la competencia para llevar a cabo trabajos de Auditoría de SI para lograr los objetivos de auditoría previstos.

5.7 El conocimiento, las habilidades y la competencia necesarios se pueden adquirir mediante una combinación de capacitación, reclutamiento y participación de recursos externos, según el plan estratégico de la EFS.

5.8 Las EFS pueden garantizar que los equipos de Auditoría de SI tengan colectivamente la capacidad de

1) Comprender los elementos técnicos de un sistema de información impulsado por TI, incluidas todas las instancias relevantes de la aplicación en uso, para poder acceder y utilizar la infraestructura de TI para el proceso de auditoría
2) Comprender las reglas existentes, las regulaciones y el entorno en el que operan los sistemas de información basados en TI de la entidad auditada
3) Comprender el mapeo de los procesos comerciales en la lógica de programación para el sistema de información de la entidad auditada
4) Aplicar los conocimientos empresariales y de TI para evaluar el riesgo de anulación manual de un programa o configuración del sistema que permita un procesamiento excepcional de las transacciones.
5) Evaluar el diseño y probar la efectividad operativa de los controles de la aplicación en los sistemas de información relevantes.
6) Comprender la metodología de la auditoría, incluidas las normas y directrices de auditoría relevantes aplicables a la EFS
7) Comprender los criterios de cumplimiento/rendimiento de TI con los que se deben comparar los resultados de la auditoría, incluidos los marcos para la gestión de SI, como COBIT, ITIL, TOGAF
8) Comprender las técnicas de SI para recopilar evidencia de auditoría de

sistemas automatizados

9) Comprender las herramientas de Auditoría de SI para recopilar, analizar y reproducir los resultados de dicho análisis o volver a realizar las funciones auditadas

10) Acceder y usar la infraestructura SI para capturar y retener evidencia de auditoría

11) Acceder y usar las herramientas de Auditoría de SI para analizar la evidencia recopilada

5.9 Las EFS pueden considerar diferentes opciones para asignar recursos humanos para trabajos de Auditoría de SI. Esto podría ser establecer un grupo central con especialistas en TI que ayuden a otros equipos de auditoría en la EFS para llevar a cabo estas auditorías o implementar especialistas en TI según los requisitos. A medida que aumenta el número de trabajos de Auditoría de SI realizados, las EFS pueden considerar establecer un grupo o función de Auditoría de SI dedicada. A este grupo se le puede confiar la responsabilidad de llevar a cabo todos los trabajos de Auditoría de SI para la EFS e interactuar con otros equipos de la EFS que tengan conocimiento heredado de la entidad auditada, a fin de obtener rápidamente una comprensión de las funciones de la entidad y los procesos comerciales relacionados. A medida que la tecnología se integra más en los sistemas de información, las EFS pueden garantizar que todos los auditores adquieran las habilidades adecuadas de Auditoría de SI.

5.10 Las EFS pueden contratar recursos externos tales como consultores de TI, contratistas, especialistas y expertos para llevar a cabo la Auditoría de SI en casos de limitaciones de recursos. Las EFS pueden garantizar que dichos recursos externos estén adecuadamente capacitados y sensibilizados a las pautas de conducta profesional y para los procesos y productos de la Auditoría de SI aplicables a la EFS, y que su trabajo sea controlado adecuadamente a través de un contrato documentado o un acuerdo de nivel de servicio y apropiada participación del personal de la EFS en las etapas de Planificación, Realización, Informes y Seguimiento de la auditoría. Por lo tanto, las EFS pueden necesitar miembros del equipo capacitados y con conocimientos internos para supervisar el trabajo de los recursos externos y hacer cumplir las directrices y los acuerdos de nivel de servicio.

5.11 Para llevar a cabo la evaluación de riesgos para los trabajos de Auditoría de SI, los principios establecidos en las SISAI 100, 200, 300 y 400 pueden ser utilizados por los auditores además de los utilizados en la realización de un tema específico de Auditoría de SI como se detalla a continuación:

1) El riesgo inherente consistiría en la probabilidad de que ciertas características de los sistemas de información impulsados por TI de una entidad auditada, por su propia naturaleza, puedan tener un impacto adverso en el cumplimiento de la función que debe cumplir la entidad. Por ejemplo, un sistema de información de una entidad auditada que debe poner a disposición información para todos los miembros del público conlleva el riesgo de rendimiento inherente que más allá de un límite máximo de usuario previsto, el sistema de información puede no responder y la información no estará disponible para cualquier usuario Si bien la entidad auditada puede adoptar controles para mitigar los riesgos inherentes, en muchos casos, la entidad puede simplemente tolerar la existencia de tales riesgos, dentro de un nivel de riesgo aceptable. El riesgo inherente puede evaluarse antes de que los auditores consideren la influencia del riesgo de control o detección.

2) El riesgo de control para un SI consistiría en la probabilidad de que los controles de TI que hayan sido adoptados por la entidad auditada no puedan mitigar el impacto adverso para el que fueron diseñados en respuesta. Por ejemplo, un sistema de información de una entidad auditada que se requiere para garantizar que el acceso a datos confidenciales, restringido al personal autorizado, puede adoptar el control de exigir la presentación de un nombre de usuario y contraseña por parte del personal que intenta obtener acceso. El riesgo de control en esta situación es que el nombre de usuario y la contraseña no son adecuadamente seguros y pueden ser adivinados por personal no autorizado a través de intentos repetidos, lo que resulta en la pérdida de confidencialidad y und posible impacto adverso en la entidad. Una entidad que insiste en el uso de contraseñas seguras y no triviales que tengan una combinación de alfabetos, números y símbolos especiales, y garantiza que el sistema de información evite el acceso al nombre de usuario más allá de un cierto número de intentos fallidos de obtener acceso. Controle el riesgo que uno que no tiene estas características.

3) El riesgo de detección consistiría en la probabilidad de que el auditor no detecte la ausencia, falla o insuficiencia de los controles de TI adoptados por una entidad, que pueden tener un impacto potencialmente adverso en la entidad.

5.12 Para llevar a cabo evaluaciones basadas en el riesgo de los sistemas impulsados por TI, las EFS pueden seleccionar una metodología que sea apropiada para su propósito. Dichas metodologías pueden variar desde simples clasificaciones del perfil de riesgo del entorno de TI de la entidad auditada como alta, media y baja en función de la comprensión de la EFS de la entidad y su entorno y el juicio profesional del equipo de Auditoría de SI de una EFS, hasta más cálculos complejos y numéricos que cuantifican la calificación de riesgo con base en datos objetivos recopilados de la entidad auditada[9].

5.13 La materialidad de una cuestión de Auditoría de SI puede decidirse bajo el marco general para decidir la materialidad en una EFS. La perspectiva de materialidad puede variar según la naturaleza del trabajo de Auditoría de SI. La materialidad para las auditorías financieras, de desempeño y cumplimiento del sector público, de las cuales se extraería el trabajo de Auditoría de SI, se ha descrito en las SISAI 100, 200, 300 y 400[10].

9 Manual de WGITA IDI sobre auditorías de TI para las Entidades Fiscalizadoras Superiores

10 Principios de auditoría financiera ISSAI 200, Principios de auditoría de desempeño ISSAI 300, Principios de auditoría de cumplimiento ISSAI 400

6 REALIZACIÓN DE AUDITORÍA DE SI

6.1 Las EFS pueden llevar a cabo auditorías de SI de acuerdo con el proceso descrito para los trabajos de Auditoría financiera (SISAI 200), Auditoría de desempeño (SISAI 300) y Auditoría de cumplimiento (SISAI 400), según sea el caso, según la naturaleza del trabajo.

6.2 Específicamente para una Auditoría de SI, los auditores pueden solicitar la debida cooperación y apoyo de la entidad auditada para completar la auditoría, incluido el acceso a registros e información. Los auditores pueden identificar el modo de acceso a los datos electrónicos en el formato necesario para permitir el análisis, en consulta con la entidad auditada. El modo de acceso a los datos sería específico de la EFS.

6.3 Antes de iniciar la evaluación de los controles en un sistema de información, los auditores pueden desarrollar una comprensión de la arquitectura del sistema y los datos subyacentes y sus fuentes para identificar las herramientas y técnicas de auditoría requeridas.

6.4 En caso de recibir volcados de datos[11] de la entidad auditada, los auditores pueden asegurarse de que cada volcado de datos vaya acompañado de una carta de la entidad auditada. Dicha carta de reenvío puede especificar

1) La fuente (mediante referencia a la marca de tiempo de generación del volcado de datos/número de hash para el volcado de datos) de los datos con el fin de garantizar la integridad de los datos, la autenticación[12] y el no repudio[13]

11 El volcado de datos se define como una gran cantidad de datos transferidos de un sistema o ubicación a otro

12 La autenticación se define como el acto de verificar la identidad de un usuario - Glosario de términos de SIACA

13 El no repudio se define como la garantía de que una parte no puede negar posteriormente los datos de origen; provisión de prueba de la integridad y el origen de los datos y puede ser verificado por un tercero - Glosario de términos

2) Los parámetros de extracción utilizados para crear el volcado de datos, es decir, consultas utilizadas/ejecución de informes.

3) Si no se recibe dicha carta de remisión de la entidad auditada, los auditores pueden generar documentos internos que indiquen información importante, como la fecha en que se entregaron los datos, de qué archivo se creó el volcado de datos y si los datos fueron del entorno de producción o de algún otro entorno, etc.

6.5 Los auditores pueden realizar una evaluación de los controles de TI (controles generales y de aplicación) adoptados por la entidad auditada, a fin de examinar su fiabilidad y suficiencia. La evaluación puede llevarse a cabo utilizando una combinación apropiada de las siguientes técnicas: entrevista, cuestionario, observación, recorrido, diagramas de flujo, captura y análisis de datos, verificación, recálculo, reprocesamiento y confirmación de terceros. El alcance de la evaluación de los controles de TI puede incluir un examen en que:

1) La política de SI ha sido definida, adoptada y comunicada

2) La estructura de gobierno de SI está en su lugar y es funcional

3) El inventario de los activos de SI se ha llevado a cabo periódicamente y se han identificado los requisitos de aumento, reemplazo y eliminación.

4) Los procesos para compartir infraestructura y servicios comunes para sistemas de información con otras entidades públicas están en su lugar y son funcionales.

5) Se han definido, adoptado y comunicado procesos para el desarrollo, adquisición y mantenimiento de sistemas de información (incluido el de gestión del cambio)

6) Se han definido, adoptado y comunicado los procesos para las operaciones de TI (contratación interna, contratación externa, acuerdos de servicio)

7) Se han adoptado medidas para garantizar la seguridad física y las condiciones físicas de trabajo previstas

8) Se han adoptado medidas para la capacitación y sensibilización de los recursos humanos para garantizar la confidencialidad, integridad y disponibilidad de la información, así como el cumplimiento de los

de SIACA

requisitos de la Política de SI y la estructura de gobierno

9) Se han adoptado medidas para garantizar la confidencialidad, integridad y disponibilidad de varios modos y canales de comunicación

10) Se han adoptado medidas para la gestión de la seguridad de la información

11) Se han adoptado medidas para la gestión de cumplimiento legal

12) Se han adoptado medidas para la continuidad del negocio y la gestión de recuperación de desastres

13) Los controles de aplicación adoptados dentro de cada sistema de información son adecuados y confiables. Dicha evaluación puede incluir la identificación de componentes significativos de la aplicación, la identificación de la importancia de la aplicación para la entidad, la revisión de la documentación disponible, la entrevista al personal, la comprensión de los riesgos de control de la aplicación y su impacto en la entidad, y el desarrollo de pruebas para examinar la adecuación y confiabilidad de tales controles de aplicación.

6.6 La evaluación de los controles generales y de aplicación puede, por lo tanto, cubrir las políticas, procesos, personas y sistemas de la entidad auditada, en línea con los objetivos de la Auditoría de SI.

6.7 Dependiendo del objetivo de la auditoría, los auditores pueden estar interesados en el diseño, implementación y efectividad operativa de los controles. Cuando el auditor se ocupa del diseño del control, una entrevista o inspección de las reglas comerciales documentadas puede ser suficiente. Cuando el auditor está preocupado por la implementación de los controles, la investigación puede no ser suficiente y puede ser necesario realizar un recorrido o realizar un análisis de datos para corroborar que el control tal como fue diseñado ha sido implementado. Finalmente, si el auditor está preocupado por la efectividad operativa del control, se le puede pedir que pruebe una muestra de transacciones para demostrar que el control ha operado efectivamente durante todo el período relevante.

6.8 Los auditores también pueden considerar cómo la evidencia sobre los controles

generales impacta la naturaleza, el momento y el alcance de la evidencia requerida para obtener seguridad sobre la operación de los controles de la aplicación. Si el Auditor ha obtenido evidencia de auditoría suficiente y apropiada con respecto a la efectividad de los controles generales que respaldan el acceso lógico del personal a los sistemas de TI y la gestión de cambios dentro del entorno de producción, puede llegar a una conclusión sobre la efectividad operativa de la automatización procedimientos de control de aplicaciones. Esto se puede hacer probando una muestra más pequeña de transacciones porque la efectividad del entorno general de TI proporciona evidencia al auditor sobre la efectividad del control de la aplicación en el período relevante. En el caso de los procedimientos de control de aplicación manual, los auditores pueden tener que probar un tamaño de muestra apropiado para el nivel de confianza seleccionado.

6.9 En función de la evaluación de los controles de TI, los auditores pueden identificar áreas prioritarias para realizar pruebas sustantivas, lo que implica pruebas detalladas de los controles de TI mediante el uso de diversas técnicas de auditoría asistida por computadora (CAAT, por sus siglas en inglés) para la investigación, extracción y análisis de datos. Los auditores pueden diseñar y ejecutar pruebas sustantivas para sustanciar los objetivos de la auditoría. Los auditores pueden seleccionar las CAAT apropiados, según sus requisitos.

6.10 Los auditores pueden usar las CAAT para ejecutar técnicas de Auditoría de SI, tales como análisis de registros de usuario, informes de excepciones, totalización de campo inteligente, comparación de archivos, estratificación, muestreo, verificaciones duplicadas, detección de brechas, envejecimiento, cálculos de campo virtual, etc. Las ventajas del uso de los CAAT incluyen análisis de grandes volúmenes de datos, repetibilidad de pruebas en diferentes conjuntos de datos y con diferentes criterios y documentación automatizada de pruebas de auditoría y resultados con marcas de tiempo.

6.11 Los auditores pueden no estar siempre en condiciones de examinar todas las instancias, transacciones o módulos o sistemas de TI, dadas las limitaciones de recursos y las compensaciones de costo-beneficio del ejercicio de auditoría. En tal situación, las EFS pueden, basándose en consideraciones de importancia relativa, adoptar un muestreo de auditoría para un examen detallado para extraer conclusiones de auditoría razonables. Las EFS pueden usar las CAAT apropiadas para llevar a cabo diferentes tipos de muestreo y determinar un tamaño de muestra apropiado,

dependiendo de los riesgos inherentes y de control subyacentes. Las muestras de auditoría[14] se extraen para proporcionar al auditor una base razonable sobre la cual extraer conclusiones sobre toda la población de datos, sobre la base de conclusiones extraídas de la aplicación de procedimientos y análisis de auditoría a la muestra de auditoría. Los auditores pueden considerar el propósito del procedimiento de auditoría y las características de la población de la que se extraerá la muestra, y determinar un tamaño de muestra suficiente para reducir el riesgo de muestreo dentro de un nivel aceptable. La auditoría en un entorno de TI puede facilitar el análisis del 100 % de una población, especialmente en la etapa de evaluación preliminar. Sin embargo, para llevar a cabo pruebas sustantivas, pueden ser necesarias muestras. Al realizar un muestreo dentro del alcance de una auditoría financiera, los auditores de SI pueden aplicar ISSAI 2530 para la selección de la muestra.[15]

6.12 Los auditores pueden asegurarse de que la evidencia electrónica recopilada y documentada sea suficiente, confiable y precisa para sostener las observaciones de la auditoría. Dicha evidencia electrónica puede consistir en archivos de datos, registros de usuarios, modelos analíticos, informes de sistemas de información de gestión, etc., y puede recopilarse y almacenarse de manera apropiada de manera tal que estén disponibles para garantizar la precisión y validez del proceso de auditoría. La evidencia reunida durante una Auditoría de SI puede tener las marcas de tiempo y detalles necesarios que contienen los pasos del análisis de datos llevado a cabo, para que quede claro cuándo se creó, almacenó y modificó por última vez, para mitigar el riesgo de cambios posteriores.

6.13 La documentación de la Auditoría de SI puede conservarse y protegerse de cualquier modificación y eliminación no autorizada. Las EFS pueden desarrollar nuevos estándares para la retención de la documentación de Auditoría de SI o adaptar los estándares existentes para cumplir con los requisitos de retención de la documentación relacionada con la Auditoría de SI. El período de retención al que se llegue sería una función del mandato de la EFS individual y los estatutos que rigen sus actividades. Se puede prestar especial atención a los medios, el formato, la esperanza de vida y los requisitos de almacenamiento de estos datos, para garantizar que los datos sean legibles dentro del marco de tiempo definido en la política de archivo y retención de datos de cada EFS. Esto puede requerir la conversión de datos de un formato a otro para mantenerse al día con los avances tecnológicos y la

14 ISSAI 2530, Auditoría Financiera, muestreo de auditoría, Secciones 6 a 9.
15 ISSAI 2530, Auditoría Financiera, muestreo de auditoría, Secciones 6 a 9.

obsolescencia.

6.14 En caso de examen de los Informes técnicos preparados por auditores externos sobre temas específicos de la tecnología, los auditores pueden adoptar los procedimientos apropiados para asegurarse de los aspectos de cumplimiento, financieros o de desempeño de dichos Informes.[16] Si, como resultado de tales procedimientos, se confía en el contenido de dichos informes, el hecho de la confianza puede divulgarse adecuadamente.

6.15 Las ISSAI estipulan que los auditores deben establecer una comunicación efectiva durante todo el proceso de auditoría y mantener informada a la entidad auditada sobre todos los asuntos relacionados con la auditoría (cf. ISSAI 100, párrafo 43). En las auditorías que involucran el trabajo de Auditoría de SI, el resultado de la Auditoría de SI puede comunicarse en algunos casos a la entidad a través de una carta separada. En estos casos, puede ser importante explicar cómo el resultado del trabajo de auditoría se relaciona con otras comunicaciones que son parte de la misma auditoría financiera, de desempeño o de cumplimiento y cómo los resultados del trabajo de Auditoría de SI pueden ser relevantes para el informe resultante de la auditoría de EFS.

16 Cuando el alcance está dentro de la auditoría financiera, los auditores pueden usar las consideraciones de auditoría ISSAI 2402 relacionadas con una entidad que usa una organización de servicios

7

INFORMES SOBRE AUDITORÍA DE SI

7.1 Dado que un trabajo de Auditoría de SI sería una Auditoría Financiera (ISSAI 200), Auditoría de Desempeño (ISSAI 300) y Auditoría de Cumplimiento (ISSAI 400), los auditores pueden considerar los requisitos de presentación de informes en consecuencia. Esto sería específico de SAI. De manera similar, cada EFS puede tener sus propios umbrales de informes basados en la materialidad de los resultados de la auditoría. Del mismo modo, un auditor, mientras informa sobre un trabajo de Auditoría de SI, puede considerar las limitaciones legales e internas sobre la divulgación de información financiera y técnica.

7.2 Los auditores pueden ser conscientes de la necesidad de limitar el uso de la jerga técnica y de la sensibilidad de la información presentada (por ejemplo, contraseñas, nombres de usuario, ID e información personal) en el informe. A pesar de la naturaleza técnica de una Auditoría de SI, los auditores pueden asegurarse de que el informe sea completamente comprensible por la alta gerencia de la entidad auditada, las partes interesadas y el público en general. Los auditores pueden incorporar un glosario de términos adecuadamente detallado en los informes, que hace referencia cruzada a la definición de un acrónimo o un término con una explicación basada en el escenario de cómo funciona esto en un entorno controlado.

7.3 Los auditores pueden considerar el posible impacto negativo del informe una vez que se publica el informe de Auditoría de SI. Por ejemplo, si el informe de Auditoría de SI detecta algunos riesgos de seguridad en el sistema de información de una entidad auditada y los mismos se informan antes de que se adopten los controles necesarios para mitigar los riesgos, la vulnerabilidad del sistema de información puede estar expuesta al público. En tal escenario, los

auditores pueden considerar opciones tales como informar solo después de que se hayan adoptado los controles necesarios, o no informar el riesgo de seguridad exacto en su totalidad, para evitar un posible impacto adverso en la entidad auditada.

8

HACER UN SEGUIMIENTO

8.1 Dado que un trabajo de auditoría en Sistemas de Información se extrae de uno o más de los principales tipos de auditoría, los auditores pueden considerar que los requisitos de seguimiento para dichos trabajos de auditoría estén a la par con los de Auditoría Financiera (ISSAI 200), Auditoría de Desempeño (ISSAI 300) y Auditoría de Cumplimiento (ISSAI 400).