Guía práctica de fiscalización dos OCEX

GPF-OCEX 5300: Directrices de auditoría de tecnoloxías da Información

Referencia: ISSAI 5300 Directrices sobre auditoría de TI, aprobada no XXII INCOSAI, en decembro de 2016

Documento elaborado pola Comisión Técnica dos OCEX e aprobado pola Conferencia de Presidentes de ASOCEX o 29/05/2017

Notas da CT-OCEX:

A ISSAI 5300 foi aprobada no XXII INCOSAI. A versión oficial española contén varios erros graves de tradución desde o orixinal inglés (probablemente atribuíbles a unha tradución automática non revisada e corrixida) que se trataron de emendar nesta versión. Aproveitouse para corrixir tamén algúns termos e homoxeneizalos cos utilizados nas ISSAI-ES (por exemplo valoración de riscos en lugar de avaliación de riscos, etc). Non obstante a base do presente documento segue sendo a versión oficial española. En caso de dúbida sobre o significado dalgunha expresión, recoméndase consultar a versión inglesa da ISSAI 5300.

Onde pon EFS debe entenderse tamén OCEX.

As referencias ás ISSAI deben entenderse feitas ás ISSAI-ES ou GPF-OCEX segundo proceda.

PREFACIO

A serie 5300-5399 das ISSAI foi asignada ás Directrices sobre Auditoría de Tecnoloxía da Información no marco destas normas internacionais. A ISSAI 5300, primeira na serie ISSAI 5300, é de alcance global e contén principios xerais sobre os fundamentos da auditoría de TI. Aborda os principios, o enfoque e a metodoloxía xeral para realizar este tipo de auditorías.

A ISSAI 5300 tamén busca servir como unha guía para que as EFS poidan levar a cabo auditorías de TI, desenvolver a capacidade de auditoría de TI e utilizar os recursos limitados de auditoría de TI, a fin de proporcionar unha garantía ás entidades auditadas, ao goberno e ao pobo dun país en materia de integridade, confiabilidade e relación prezo-calidade en implementacións de TI.

A ISSAI 5300 desenvolveuse no marco das ISSAI, mediante a realización dunha revisión das normas existentes en relación coas auditorías de TI/Auditorías de Sistemas de Información, as normas relativas aos sistemas de información, as normas nacionais e internacionais de auditoría, en particular, as ISSAI existentes. Outra característica clave da ISSAI 5300 é que asegura que a natureza básica inherente ás auditorías de TI estea vinculada/integrada adecuadamente, coas diferentes formas de auditoría identificadas nas ISSAI nivel 3.

Ademais, ao ser unha orientación nivel 4, o material nesta ISSAI dividiuse en dúas categorías: **Requirimentos** - elementos esenciais para a realización dunha auditoría de TI de boa calidade; seguido por **Explicacións** - que interpretan e definen os requirimentos en termos máis xerais. Isto fíxose para asegurar que a ISSAI conserve a súa función principal de proporcionar orientación e apoio xeral como está previsto no marco das ISSAI.

A ISSAI 5300 tamén ten en conta os niveis de madurez dos sistemas de información no sector gobernamental e o nivel de madurez das auditorías de TI en diferentes EFS.

Esta ISSAI estrutúrase nos seguintes subtemas principais:

1. Marco para as auditorías de TI;
2. Requirimentos xerais especificamente relacionados coas auditorías de TI;
3. Requirimentos específicos para o proceso de auditoría de TI;
4. Técnicas e ferramentas de auditoría de TI;
5. Requirimentos de información das auditorías de TI.

É importante destacar que existe un anexo dedicado á análise de datos.

Esta ISSAI senta as bases para o desenvolvemento futuro das ISSAI da serie 5300-5399 e/ou de guías sobre materias específicas, de interese para a comunidade da INTOSAI no ámbito das auditorías de TI.

A elaboración deste traballo estivo a cargo dun equipo composto polas EFS de Brasil, India (xefe de proxecto), Indonesia, Xapón, Polonia e os EE.UU, EFS que estivo a cargo da súa redacción.

A. MARCO PARA A AUDITORÍA DE TI

1. Mandato e alcance da ISSAI 5300

1.1 A ISSAI 5300 establece o marco xeral para a realización das auditorías de TI no marco das ISSAI.

1.2 O marco establecido nesta ISSAI é coherente cos Principios Fundamentais de Fiscalización do Sector Público (ISSAI 100), os Principios Fundamentais da Auditoría Financeira (ISSAI 200), os Principios fundamentais da Fiscalización Operativa (ISSAI 300) e os Principios Fundamentais da Auditoría de Cumprimento (ISSAI 400).

1.3 Este proxecto de ISSAI define os requirimentos para a práctica profesional da auditoría de TI, seguidos de explicacións para mellorar a claridade e facilidade de lectura do marco.

1.4 Os requisitos conteñen información necesaria para un traballo de alta calidade en materia de auditoría de TI. Estes permiten que os auditores saiban o que se espera deles e que os grupos de interese saiban o que poden esperar da auditoría de TI realizada por unha EFS.

1.5 As explicacións describen con máis detalle o que significa un requisito ou o que tenta abarcar.

1.6 Este proxecto de ISSAI foi preparado por un equipo de proxecto composto polas EFS de Xapón, Polonia, Indonesia, India, os EE.UU. e Brasil.

2. Introdución ás Auditorías de TI

2.1 As entidades gobernamentais adoptaron cada vez máis as tecnoloxías da información e a comunicación (TIC) para levar a cabo as súas funcións e ofrecer diversos servizos. Tales sistemas baseados no TIC son comunmente coñecidos como Sistemas de Información (SE) ou Sistemas de Tecnoloxía da Información (TI).

2.2 As Entidades Fiscalizadoras Superiores (EFS) teñen o mandato de auditar ao Goberno e as súas entidades, de acordo co seu respectivo mandato de auditoría.[1]

2.3 As EFS, polo tanto, promoven a eficiencia, a rendición de contas, a eficacia e a transparencia da administración pública[2].

2.4 O desenvolvemento continuo da tecnoloxía da información e a comunicación fixo posible capturar, almacenar, procesar e entregar información en forma electrónica. Esta transición cara ao procesamento electrónico provocou un cambio significativo na contorna no que traballan as EFS. Por outra banda, o gasto do goberno en TI está a crecer, por tanto faise imperativo para as EFS desenvolver a capacidade adecuada para levar a cabo as auditorías de TI.

3. Definición de auditoría de TI

3.1 As auditorías de TI defínense como:

"Un exame e revisión dos sistemas de TI e controis relacionados que busca obter seguridade ou identificar violacións aos principios de legalidade, eficiencia, economía e eficacia do sistema de TI e os seus controis relacionados."

3.2 Auditoría de TI[3] é por tanto, un termo amplo que abarca as auditorías financeiras[4] (para avaliar a exactitude e o cumprimento das manifestacións realizadas nos estados financeiros dunha organización), as auditorías de cumprimento[5] (avaliación dos controis internos), e as auditorías operativas[6] (para avaliar se os sistemas de TI satisfán as necesidades dos usuarios e non someten á entidade a riscos innecesarios). Con todo, pode haber casos en que algunhas auditorías só se destinen a avaliar un determinado compoñente TI dun sistema.

[1] ISSAI 1, Declaración de Lima

[2] Resolución da Asemblea Xeral das Nacións Unidas A/66/209

[3] A auditoría de TI tamén se coñece como auditoría de SI, auditoría de sistemas, auditoría da información, auditoría de seguridade da información, revisión de aseguramento informático, aseguramento de TI, etc.

[4] ISSAI 200 Principios Fundamentais da Auditoría Financeira

[5] ISSAI 400 Principios Fundamentais da Fiscalización de Cumprimento.

[6] ISSAI 300 Principios Fundamentais da Fiscalización Operativa.

4. Mandato para as auditorías de TI

4.1 O mandato da EFS para executar auditorías de TI derívase do mandato xeral da EFS para realizar auditorías.[7] Algunhas EFS tamén poden ter un mandato específico para a realización de auditorías de TI ou auditoría dos sistemas de TI.

4.2 Para moitas EFS, o mandato para realizar auditorías financeiras, auditorías operativas, e auditorías de cumprimento será mandato suficiente para levar a cabo as auditorías de TI. Isto débese a que os sistemas de TI apoian as principais operacións dunha entidade, que poden incluír os sistemas financeiros. Polo tanto, a execución de auditorías de TI pode non requirir mandatos adicionais.

4.3 O mandato específico, se se proporciona, debe definir o alcance da auditoría para auditar sistemas de TI, que son utilizados pola entidade para cumprir os seus obxectivos funcionais. Tamén debe proporcionar un acceso oportuno, ilimitado, directo e libre a todos os documentos necesarios e a información da entidade[8], tanto físicos como electrónicos, xa sexa se a función ou calquera das súas partes é realizada por persoal interno ou subcontratado.

4.4 O mandato da EFS para levar a cabo as auditorías de TI debe axustarse aos principios contidos nas ISSAI dos niveis 1 e 2.

B. REQUIRIMENTOS XERAIS ESPECIFICAMENTE RELACIONADOS COAS AUDITORÍAS DE TI

5. Enfoque de auditoría baseada en riscos da Auditoría de TI

Requirimento:

O auditor deberá considerar os riscos da auditoría de TI cando tome un risco baseado no enfoque, método ou modelo de auditoría.

As auditorías de TI deberán levar a cabo sobre a base dun enfoque de auditoría baseada en riscos

Explicación:

5.1 O enfoque de auditoría baseada en riscos implica a identificación dos elementos[9] de risco na entidade que está a ser avaliada xunto co seu impacto potencial e, a partir de aí, a identificación de áreas prioritarias a ser auditadas.

5.2 Os riscos presentes durante a realización da auditoría dunha entidade, implican riscos inherentes, de control e de detección. Os elementos do risco identifícanse abordando os tres riscos mencionados. Xuntos, estes constitúen o que se chama o risco de auditoría.

5.3 Os riscos inherentes son aqueles que forman parte do sistema e que poden ter impacto sobre o cumprimento do mandato encomendado á entidade. O anonimato dos usuarios é un risco inherente dun sistema de TI, especialmente nunha contorna interconectada. As organizacións deberían establecer medidas de control para abordar os riscos inherentes. Nalgúns casos, a entidade pode mesmo aceptar os riscos como tal - sen ningún tipo de medidas de resposta para facerlles fronte - cando se determina que o seu impacto non é significativo e, por tanto, está dentro dun nivel de risco aceptable.

5.4 Os riscos de control son aqueles onde as medidas de control poden eventualmente fallar. En tales casos, é posible que xurdan erros materiais, que deberían ser identificados inmediatamente. Os sistemas de TI sempre abordan estes a través de Controis de Aplicación[10] e Controis Xerais[11]. É a robustez destes

[7] Principio 3, ISSAI 10 - Declaración de México sobre a Independencia das EFS e as ISSAI 100 - Principios fundamentais de Fiscalización do Sector Público.

[8] Acceso sen restricións aos rexistros; Principio 4, ISSAI 10 - Declaración de México sobre a independencia das EFS.

[9] Os elementos de risco estarían relacionados con áreas como gobernanza de TI, deseño e desenvolvemento do sistema, contratación interna/externa, as operacións, seguridade TI, monitoreo e control.

[10] Os controis de aplicación son os controis incorporados nunha aplicación individual ou un grupo de aplicacións relacionadas que comprenden un sistema de aplicación de TI. Hai controis de entrada, controis de procesamento, controis de saída e controis de datos mestres, que son aplicables ás etapas de entrada, procesamento e saída do sistema de TI.

[11] Os controis xerais son controis sobre os sistemas e procesos relacionados que apoian o sistema de aplicación de TI. Estes refírense a áreas como a razón comercial do sistema de TI, deseño e desenvolvemento de sistemas, adquisicións, contratación externa/interna, as operacións (á parte dos controis de aplicación), xestión de recursos humanos, seguridade

controis o que garante o cumprimento da función propia da organización/sistema de TI. O fracaso ou a posta en perigo destes controis constitúen unha situación de risco de control.

5.5 Os riscos de detección na realización das auditorías de TI son os riscos de non detectar a ausencia ou o fallo de TI e dos seus controis relacionados, así como o risco asociado co funcionamento do sistema TI.

5.6 Existen moitos enfoques de valoración de riscos e metodoloxías dispoñibles que a EFS pode elixir. Estas van desde simples clasificacións do perfil de risco dos sistemas de TI como alto, medio e baixo, baseadas no criterio dos auditores TI dunha EFS, a cálculos complexos e, aparentemente científicos que proporcionan unha cualificación numérica de riscos dos sistemas de TI.[12]

6. Materialidade

Requirimento:

A EFS deberá considerar a materialidade en todas as etapas do proceso de auditoría de TI.

Explicación:

6.1 Os auditores de TI deberán considerar a materialidade durante todo o proceso de auditoría (TI). As consideracións referentes á materialidade afectan as decisións relacionadas coa natureza, momento de realización e extensión dos procedementos de auditoría, así como a avaliación dos resultados da auditoría. As consideracións poden incluír as preocupacións das partes interesadas, o interese público, os requisitos regulamentarios e as consecuencias para a sociedade.[13]

6.2 A materialidade refírese a todos os aspectos destas auditorías, tales como a selección dos temas, a definición dos criterios, a avaliación da evidencia e a documentación, así como tamén a xestión dos riscos de producir ou obter achados e informes inadecuados ou de baixo impacto.

6.3 A materialidade dunha auditoría de TI debería ser decidida baixo o marco xeral dunha decisión a nivel de EFS. A perspectiva da materialidade variará dependendo da natureza da auditoría de TI. A materialidade relativa a auditorías financeiras, de desempeño e cumprimento do sector público, das cales as auditorías de TI forman parte, discútese nas ISSAI 200, 300 e 400[14].

6.4 Materialidade e Risco

A valoración de riscos utilizada na auditoría de TI está intimamente ligada aos requisitos de materialidade das auditorías. A materialidade dun incumprimento avalíase con base na capacidade de influír nas decisións dos usuarios. Cando os riscos inherentes son altos, a aparición dun pequeno incumprimento pode ser significativo debido á posibilidade de que o efecto de tal incumprimento posúa unha natureza acumulativa. Cando os riscos de control son altos (é dicir, existe ausencia/fallo dos controis necesarios para os riscos identificados), de maneira similar, un pequeno incumprimento será significativo pola posibilidade de que o efecto de tal incumprimento posúa unha natureza acumulativa.

6.5 Os auditores de TI non están sempre en condicións de examinar todas as instancias / transaccións / módulos ou sistemas, dadas as limitacións de recursos e o custo-beneficio do exercicio de auditoría. En tal situación, os auditores de TI poden recorrer á identificación da materialidade e a adopción da mostraxe de auditoría para un exame detallado, a fin de sacar conclusións de auditoría razoables. Pódese recorrer ao uso de ferramentas de TI na realización de diferentes tipos de mostraxe. Os niveis de riscos inherentes e de riscos de control poden impactar no tamaño da mostra. A maior risco inherente ou risco de control, maior deberá ser o tamaño da mostra.

---

de TI, monitoreo, etc. Os controis xerais e os controis de aplicación están asociados intimamente, asegurando ao mesmo tempo a implementación exitosa dun sistema informático. Se os controis xerais son débiles, diminúen considerablemente a fiabilidade dos controis asociados coas aplicacións de TI individuais.

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

[13] ISSAI 100 - Principios Fundamentais de Fiscalización do Sector Público - Parágrafo 41.

[14] ISSAI 200 - Principios Fundamentais da Auditoría Financeira, ISSAI 300 - Principios Fundamentais da Fiscalización Operativa, ISSAI 400 - Principios Fundamentais da Fiscalización de Cumprimento.

7. Documentación

Requirimento:

A EFS manterá suficiente documentación do proceso de auditoría de TI e os seus resultados para garantir que calquera auditor experimentado alleo á auditoría poida replicala.

O auditor deberá preparar unha documentación de auditoría que sexa completa e detallada a fin de proporcionar unha comprensión global da auditoría.

A revisión da documentación debe permitirlle a calquera outro auditor de TI chegar ás mesmas conclusións de auditoría.

Explicación:

7.1 Os requisitos xerais de documentación nunha auditoría de TI son esencialmente aqueles descritos nas ISSAI de nivel 3, a saber: ISSAI 100, 200, 300 e 400. Estes tamén se aplicarían a unha auditoría de TI. Con todo, a natureza das auditorías de TI pode necesitar axustes específicos no proceso de documentación.

7.2 O rol da documentación nunha auditoría de TI é permitir comprender a planificación e execución da auditoría, que traballo levou a cabo para apoiar os achados e conclusións, e as recomendacións da auditoría. A documentación debe ser o suficientemente detallada como para permitir que un auditor de TI con experiencia, sen coñecemento previo da auditoría, entenda a natureza, oportunidade, alcance e resultados dos procedementos realizados de conformidade coas ISSAI pertinentes, normas nacionais e requisitos legais e regulamentarios aplicables. A evidencia obtida, que serve de apoio ás conclusións e recomendacións da auditoría, ao razoamento detrás de todas as materias importantes que requiren o exercicio dun xuízo profesional e as consecuentes conclusións, tamén deben ser documentadas, de modo que sexa fácil de entender por un auditor de TI con experiencia. A documentación debe ser fiable, de maneira que non exista desacordo sobre o contido da documentación coa entidade auditada.

7.3 A documentación nunha auditoría de TI xoga un papel importante para asegurar que cada paso do proceso de auditoría e cada achado sexa mapeado ou referenciado a un punto específico do cumprimento ou incumprimento das normas ou regulacións aplicables.

7.4 Do mesmo xeito que en calquera outra auditoría, se calquera achado no transcurso dunha auditoría non é coherente coa conclusión xeral da auditoría relativa a unha materia importante ou hai un desacordo coa entidade auditada sobre as conclusións da auditoría, entón, os auditores de TI teñen que documentar a forma en que abordaron aquela inconsistencia e/ou desacordo.

7.5 Formato da documentación de auditoría de TI

A documentación da auditoría de TI inclúe formatos de papel e persoais electrónicos para rexistrar información sobre o sistema de TI auditado, os detalles das reunións mantidas coa dirección e dentro do equipo de auditoría, os achados de auditoría, e as probas das conclusións da auditoría. Non hai un formato estándar para a documentación da auditoría de TI nas ISSAI. Polo demais, os formatos poden diferir entre as diferentes EFS. É posible que haxa certo grao de estandarización dentro de cada EFS en termos de checklists , modelos, organización de papeis de traballo, etc.

7.6 Conservación da documentación de auditoría de TI

A documentación de auditoría de TI debe ser conservada e protexida de calquera modificación e eliminación non autorizada. Cada EFS pode desenvolver novas normas para o resgardo da documentación de auditoría de TI ou adaptar as normas existentes para satisfacer os requisitos de conservación da documentación relativa a auditoría de TI. O período de almacenamento así definido, sería unha función do mandato da EFS individual e do estatuto que rexe as súas actividades.

Débese prestar especial atención ao soporte, o formato, a vida útil e os requisitos de almacenamento destes datos, para asegurar que estes sexan lexibles dentro do prazo definido na respectiva política de almacenamento e retención de datos de cada EFS. Isto pode requirir a conversión dos datos dun formato a outro para manterse ao día cos avances tecnolóxicos e a obsolescencia.

8. Competencia

Requirimento:

A EFS deberá asegurarse de que o equipo de auditoría estea composto por membros que posúen colectivamente as competencias para realizar a auditoría de TI de acordo coas normas.

Explicación:

8.1 Os coñecementos, habilidades e competencias necesarias poderían adquirirse a través dunha combinación de capacitación, selección de persoal novo e contratación de recursos externos de acordo co plan estratéxico da EFS.

C. REQUIRIMENTOS RELACIONADOS CO PROCESO DE AUDITORÍA DE TI

9. Planificación de auditorías de TI

Requirimento:

A EFS debe planificar unha auditoría de TI baseada na valoración de riscos.

Explicación:

9.1 A planificación da Auditoría de TI por parte dunha EFS, pode levar a cabo de acordo cos mandatos lexislativos, solicitudes lexislativas / executivas, ou por iniciativa propia.

9.2 Planificación de auditoría nas EFS baseada na valoración de riscos

As EFS poden planificar auditorías mediante unha selección baseada na valoración de riscos. Neste proceso a EFS prioriza e selecciona as auditorías que levarán a cabo, sobre a base dunha valoración de riscos. A planificación dunha auditoría de TI baseada no risco pódese levar a cabo en tres niveles - Estratéxico, Anual, e de Equipo, que estarán suxeitos ao plan estratéxico xeneral da EFS. Con todo, unha EFS pode decidir por unha mestura dun ou máis destes niveis, como polos seus recursos e requisitos de auditoría, baseados na análise de risco.

Figura 1: Xerarquía de planificación de auditoría típica para as EFS

10. Planificación estratéxica de auditoría de TI

Requirimento:

O plan estratéxico dunha EFS deberá posuír un compoñente que oriente a auditoría de TI e os seus requirimentos asociados.

A EFS deberá desenvolver o Plan estratéxico de auditoría de TI de acordo co plan estratéxico xeral de auditoría.

Explicación:

10.1 O plan estratéxico de auditoría de TI contén as metas e os obxectivos da auditoría dos sistemas de TI nas entidades públicas sometidas ao control dunha EFS. O plan elabórase normalmente por un período de entre 3-5 anos, reflectindo a evolución da contorna de TI e a súa adopción por parte das entidades públicas. O plan estratéxico para a auditoría dos sistemas de TI debe estar aliñado co plan estratéxico xeral da EFS.

10.2 As EFS teñen por obxectivo garantir a transparencia, a rendición de contas e a contribución á boa gobernanza, en consonancia coa súa visión, misión e valores. Como tal, o seu plan estratéxico ou obxectivos deberían abordar o desenvolvemento institucional, o desenvolvemento do sistema organizacional e o desenvolvemento da capacidade profesional, segundo sexa necesario, en resposta á consecución das súas metas estratéxicas. Para as auditorías de TI, as EFS poden avaliar a súa contorna a través de enquisas, a interacción coas entidades auditadas, a avaliación da dirección e o desenvolvemento de solucións tecnolóxicas e as súas adopcións por parte das entidades auditadas, e calquera outro requisito legal ou obrigatorio.

10.3 A identificación do universo de auditoría nesta etapa será relevante. As EFS poderán identificar as súas prioridades de auditoría en resposta á avaliación da súa contorna e o universo de auditoría, e decidir sobre as súas metas e obxectivos estratéxicos. Para lograr os seus obxectivos xerais, a través dos medios e recursos limitados dispoñibles, o plan de implementación estratéxica da EFS pode incluír a identificación das necesidades relacionadas co desenvolvemento institucional, o que incluirá o mandato e o marco legal que permiten á EFS a realización de auditorías de TI, o desenvolvemento de sistemas organizacionais para establecer sistemas e procedementos na EFS, a fin de levar a cabo as auditorías de TI e o desenvolvemento da capacidade profesional para adquirir as habilidades e capacidades necesarias para poder levar a cabo as auditorías de TI.

10.4 Planificación de auditoría baseada en riscos

A planificación de auditoría baseada en riscos implica abordar os elementos de risco que terán impacto sobre a relevancia das auditorías e a precisión das conclusións de auditoría elaborados como resultado da mesma. A valoración do risco a nivel de planificación estratéxica de auditoría de TI aborda a cuestión da relevancia das auditorías de TI con respecto ao obxectivo estratéxico global das EFS de asegurar a boa gobernanza, a transparencia e a rendición de contas na xestión pública.

10.5 Deberá realizarse unha revisión periódica e actualización do plan estratéxico da EFS para abordar os obxectivos de garantir a transparencia, a rendición de contas e a contribución á boa gobernanza.

10.6 Pódese facer referencia ás ISSAI, especialmente, á ISSAI 100 - Principios Fundamentais de Fiscalización do Sector Público - para abordar as cuestións relacionadas coa planificación estratéxica dunha EFS.

11. Planificación anual de auditoría de TI

Requirimento:

O plan anual de auditoría de TI debe estar de acordo co plan estratéxico de auditoría de TI.

O plan anual de auditoría de TI debe cubrir os asuntos de importancia incluídos no plan estratéxico de auditoría de TI de acordo coa prioridade determinada a través da valoración de riscos.

Explicación:

11.1 A elaboración do plan anual de auditoría de TI debe estar aliñado co plan estratéxico de auditoría de TI. Esta etapa da planificación implica a selección do sistema de TI ou entidade a ser auditada.

11.2 No marco do plan estratéxico de auditoría de TI dunha EFS, pódese utilizar un enfoque baseado en

riscos para priorizar e seleccionar os temas adecuados. Isto implicará a creación e uso dun inventario de organizacións / sistemas de TI auditables, xunto con criterios claves para levar a cabo a valoración de riscos. Este inventario pode ser tamén o universo de auditoría identificado durante a etapa de Planificación Estratéxica, pero con detalles específicos sobre o tipo e a descrición dos sistemas de TI /entidades a ser utilizados na avaliación do seu perfil de risco. Un marco de valoración de riscos desenvolvido polas EFS pode utilizarse posteriormente para finalizar unha selección de auditoría.

11.3 Ademais dun enfoque baseado no risco na selección dos temas de auditoría, moitas EFS asumen auditorías por mandato da lei e por solicitudes dos órganos lexislativos ou o Executivo.

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

Requirimento:

O plan de auditoría de TI a nivel de equipo deberá estar de acordo coa valoración de riscos no plan anual de auditoría de TI.

O plan de auditoría de TI a nivel de equipo deberá cubrir as materias das áreas de risco significativo identificadas no plan anual de auditoría de TI e incluír un programa detallado de auditoría.

Explicación:

12.1 Este nivel implica o desenvolvemento dun programa de auditoría detallado, comezando coa descrición dos obxectivos da auditoría de TI seleccionada.

12.2 O requisito previo para o desenvolvemento do programa de auditoría é ter un coñecemento claro da entidade auditada, os seus sistemas de información, e as súas actividades de TI relacionadas.

12.3 O grao de coñecemento da entidade e os seus procesos que requiran os auditores de TI será determinado pola natureza da entidade e o nivel de detalle co que se está realizando o traballo de auditoría. O obxectivo ou a finalidade detrás da implementación dun sistema de TI deben ser identificados. O coñecemento da entidade debería incluír a actividade principal, os riscos financeiros e inherentes aos que se enfronta a entidade e os seus sistemas de TI. Tamén se debe coñecer en que medida a entidade recorre á subcontratación para cumprir cos seus obxectivos e cando completo o proceso de negocio foi trazado nunha contorna de TI[15]. O auditor debe utilizar esta información para identificar problemas potenciais, formular os obxectivos e o alcance do traballo, realizar o traballo e ter en conta as medidas de xestión para as que os auditores de TI deben estar alerta.

12.4 De acordo co enfoque de auditoría baseado no risco, os riscos de control estarán relacionados con elementos dos controis xerais e controis de aplicación de TI. A maior risco de control, maior é a necesidade de realizar máis probas substantivas.

12.5 En xeral, os auditores de TI están chamados a probar os controis relacionados coa tecnoloxía, mentres que outros auditores proban os controis financeiros, regulatorios e de cumprimento. O papel do auditor é entender o negocio potencial e os riscos de TI que enfronta a entidade auditada e, á súa vez avaliar se os controis utilizados son adecuados para cumprir o obxectivo de control. No caso dos controis xerais de TI, é importante que o auditor entenda as categorías xerais e o alcance dos controis xerais en funcionamento, avalíe a supervisión efectuada pola dirección e a sensibilización do persoal da entidade sobre este punto, e pescude cando eficaces son os controis na prestación da función prevista. Mesmo en pequenas entidades nas que os sistemas de información e procesos de negocio relevantes para a presentación de informes financeiros son menos sofisticados, o seu papel é significativo.[16] Se os controis xerais son débiles, diminúen considerablemente a fiabilidade dos controis asociados coas aplicacións de TI individuais[17]. Será importante para os auditores de TI entender a función asignada á aplicación de TI co fluxo de traballo asociado. Os auditores de TI deben ser capaces de identificar cada entrada, os

[15] As entidades que pasan dunha contorna manual a un computarizado, normalmente adoptarían un exercicio de reinxeniería de procesos de negocio (BPR). Poderíase observar que algúns dos procesos de negocio séguense levando a cabo de forma manual, xunto cunha interface cos sistemas de TI. Estes escenarios especiais presentarían áreas de interese específico para os auditores de TI.

[16] ISSAI 1315 Identificación e avaliación dos riscos de irregularidades importantes a través dunha comprensión da entidade e a súa contorna.

[17] WGITA IDI Handbook on IT Audits for Supreme Audit Institutions

procesos levados a cabo pola dita aplicación e os resultados xerados desta. A comprensión dos datos mestres que inflúen na entrada, o proceso e os resultados e a súa seguridade, axudará aos auditores de TI a avaliar o cumprimento do sistema de TI cos requisitos de exactitude, completitude, integridade, confidencialidade, dispoñibilidade, fiabilidade, pertinencia e cumprimento dos datos, ao longo das etapas de procesamento da información, captura e procesamento de datos e a entrega/saída de información.

12.6 Sobre a base do coñecemento adquirido do sistema de información e da entidade auditada, o auditor de TI pode decidir sobre o seu enfoque para as auditorías de TI. A auditoría de TI incluiría, eventualmente, a auditoría da gobernanza de TI, os controis xerais de TI e os controis de aplicación de TI ou unha combinación destes.

13. Selección da mostra apropiada de auditoría de TI

Unha mostra de auditoría[18] é a aplicación de procedementos de auditoría a menos do 100 por cento dos elementos dentro dun grupo ou poboación de relevancia de auditoría, de tal maneira que todas as unidades de mostraxe teñen unha oportunidade de selección, a fin de proporcionar ao auditor unha base razoable para sacar conclusións sobre toda a poboación. Isto tamén é aplicable á selección dunha mostra para a auditoría de TI. Por outra banda, cando se deseña unha mostra de auditoría, o auditor de TI deberá considerar a finalidade do procedemento de auditoría, as características da poboación da que se extraerá a mostra e as técnicas e ferramentas utilizadas para extraer a mostra e analizalas.

O auditor de TI debe determinar un tamaño de mostra suficiente para reducir o risco de mostraxe a un nivel aceptablemente baixo. O auditor de TI deberá seleccionar os elementos da mostra de tal maneira que, cada unidade de mostraxe na poboación teña unha oportunidade de ser seleccionada. Auditar nunha contorna TIC pode facilitar a análise do 100 por cento da poboación, sobre todo na fase de avaliación preliminar ***(Sección 21, a continuación)***. Con todo, para a realización de calquera proba substantiva ***(Sección 21, a continuación)*** ou exames detallados, aínda se pode requirir extraer unha mostra. Os auditores de TI poden utilizar as directrices da ISSAI 1530 ou outros procesos derivados en uso no seu EFS para a selección da mostra.[19]

14. Obxectivos da auditoría de TI

Requirimento:

Os obxectivos da auditoría de TI deben axustarse ás áreas de risco identificadas durante a planificación de auditoría de TI a nivel de equipo, dependendo do tipo de enfoque de auditoría que se contempla - auditoría financeira, de cumprimento ou operativa.

Explicación:

14.1 Os obxectivos da auditoría de TI consistirán en examinar se os procesos e recursos de TI en conxunto, logran alcanzar os obxectivos previstos pola organización para asegurar a eficacia, eficiencia e economía nas súas operacións, cumprindo coas normas existentes e equilibrando os riscos ao mesmo tempo.

14.2 Deste xeito, as auditorías de TI poderían ser auditorías do conxunto dun sistema de TI ou de dominios específicos, como son a seguridade de TI, a adquisición da solución de negocio, os controis xerais de TI, os controis de aplicación, o desenvolvemento de sistemas e a continuidade do negocio, ou outras áreas que se mencionan no Manual WGITA IDI.

14.3 A auditoría de TI atravesa transversalmente os dominios da auditoría financeira, a auditoría de cumprimento ou a auditoría operativa. As auditorías de TI poden axudar aos tres tipos de auditorías ou poden levar a cabo no contexto de calquera delas ou unha combinación delas.[20]

14.4 Obxectivos con respecto ás auditorías financeiras

A definición da auditoría financeira[21] describe as cuestións relativas á confianza, a preparación dos estados financeiros de conformidade cun marco de presentación de informes financeiros e a

[18] ISSAI 1530, Auditoría Financeira, Mostraxe de Auditoría.

[19] ISSAI 1530, Directriz de Auditoría Financeira, Mostraxe de Auditoría, Páxina 15.

[20] ISSAI 100 - "As EFS tamén poderán efectuar auditorías combinadas, incorporando aspectos financeiros, de desempeño e/ou de cumprimento.".

[21] ISSAI 200 - Principios Fundamentais da Auditoría Financeira.

presentación dos estados financeiros, conforme aos requisitos de importancia relativa. Isto cobre os obxectivos xerais relativos á garantía do sistema financeiro de cumprir co marco de presentación de informes na preparación dos estados financeiros e a presentación dos informes de resultados financeiros sen erros significativos. É necesario, polo tanto, que un sistema de TI contemple todos os requisitos para a preparación dos estados financeiros, é dicir, a captura da información financeira, a aplicación dos requisitos do marco, o procesamento da información, e a presentación no formato requirido. En termos xerais, trátase de cuestións relacionadas coa aplicación de controis de entrada, procesamento e saída, ademais dos datos mestres e a seguridade da aplicación. Con todo, os controis de aplicación son dependentes do apoio adecuado dos controis xerais de TI e a gobernanza de TI. Por tanto, os auditores financeiros deberían poder obter unha seguridade da idoneidade do sistema de TI e os seus controis asociados, antes de concluír a súa auditoría. A seguridade no sistema de TI debería ser obtida a través dunha auditoría de TI do sistema que analice todos os aspectos da gobernanza de TI, os controis xerais de TI e os controis de aplicación de TI.

Unha vez obtida seguridade tras realizar unha auditoría de TI completa, poida que non sexa esencial levar a cabo unha auditoría de TI do mesmo sistema durante cada auditoría financeira, se hai unha seguridade de que non sucedeu ningún cambio no sistema, nin estivo comprometido, durante o período desde a última auditoría de TI.

14.5 Obxectivos con respecto ás auditorías de cumprimento

A auditoría de cumprimento é a avaliación independente de se unha materia determinada é conforme coas normas e regulacións aplicables identificadas como criterios. As auditorías de cumprimento levan a cabo mediante a avaliación de se as actividades, operacións financeiras e información cumpren, en todos os seus aspectos significativos, coas autoridades que rexen á entidade auditada.

O obxectivo da auditoría de cumprimento do sector público é permitir á EFS avaliar se as actividades das entidades do sector público cumpren coas normas e regulacións que rexen estas entidades. Isto implica presentar informes sobre o grao en que a entidade auditada cumpre cos criterios establecidos. A auditoría de TI permite que se efectúe esta determinación para sistemas automatizados. A auditoría de cumprimento pode tratar sobre a regularidade (cumprimento cos criterios formais, tales como leis, regulacións e convenios relevantes) ou sobre a ética (observancia dos principios xerais que rexen unha sa administración financeira e o comportamento dos funcionarios públicos). Mentres que a regularidade é o enfoque principal da auditoría de cumprimento, a ética pode ser un asunto pertinente dado o contexto do sector público, no que existen certas expectativas relacionadas coa administración financeira e o comportamento dos funcionarios públicos e das entidades do sector público. Dependendo do mandato da EFS, o alcance da auditoría pode, polo tanto, incluír aspectos sobre ética[22].

Os obxectivos e características da auditoría de cumprimento describen a necesidade de cumprir co debido proceso, a regularidade e a ética. Tamén se require que o sistema de TI nunha entidade do sector público cumpra coas leis e regulamentos aplicables, así como as normas e directrices adoptadas pola entidade. Os auditores de TI deben avaliar o cumprimento por parte do sistema de TI de ditos regulamentos, así como das normas, directrices e diferentes parámetros rendemento da entidade para obter unha conclusión de auditoría. Toda esta avaliación levarase a cabo baseada nos criterios identificados derivados das regras, leis, normas, criterios de rendemento ou mesmo os requisitos propios da entidade. A avaliación do cumprimento en relación á gobernanza de TI, implicará garantías sobre os mecanismos para asegurar que as funcións de gobernanza estean a levarse a cabo e monitoreando periodicamente, que o mecanismo de control interno estea a funcionar eficazmente e que todas as políticas de TI estéanse aplicando conforme ao previsto. A avaliación do cumprimento en relación aos controis xerais de TI implicará a avaliación da existencia de controis cos debidos mecanismos de seguimento e mitigación de riscos implementados e a adhesión ás normas prescritas e parámetros de desempeño na entidade. A avaliación dos controis de aplicación de TI, implicará a avaliación da existencia de mapeo de procesos de negocio e regras no sistema de TI, e controis de entrada, proceso e saída relacionados coa validación de datos, integridade, exactitude e fiabilidade dos procesos.

[22] ISSAI 400 - Principios Fundamentais das Fiscalizacións de Cumprimento.

A auditoría de cumprimento por parte dun sistema de TI pode, invariablemente, requirir o uso de Técnicas de Auditoría Asistidas por Computador (CAAT) para levar a cabo a análise da información e identificar excepcións.

14.6 Obxectivos con respecto ás auditorías operativas

A auditoría operativa é unha revisión independente, obxectiva e fiable sobre se os proxectos, sistemas, operacións, programas, actividades ou entidades públicas están a operar de acordo cos principios de economía, eficiencia e eficacia e se hai marxe de mellora.

Os auditores de TI examinarán os sistemas de TI implementados con respecto aos criterios de economía, eficiencia, eficacia e valor para o cidadán.

O exame da economía en relación coa implementación de sistemas de TI implica esencialmente a minimización dos custos dos recursos ao longo do ciclo de vida do sistema de TI, desde a adquisición do sistema á implementación do mesmo e o seu funcionamento regular. En caso da externalización dalgunha función, o custo de dita externalización debe ser minimizado. Unha das mellores maneiras de minimizar estes custos é a través dunha análise do mercado. Con todo, a definición ineficiente de requirimentos de usuario debido a un coñecemento inadecuado dos requisitos por parte da entidade, pode obstaculizar tal enfoque e dar lugar a maiores custos. A avaliación da posibilidade de que os servizos de TI externalizados puidesen ser levados a cabo cos recursos dispoñibles, indicará un uso ineficiente dos recursos. Polo tanto, durante a auditoría operativa de adquisicións de TI, os auditores de TI poderían pór énfases nas limitacións da entidade ou o proceso de adquisición, segundo sexa o caso.

O exame da eficiencia en relación á implementación dos sistemas de TI implicaría aumentar ao máximo a utilización dos recursos ou reducir ao mínimo a súa utilización ineficiente, mantendo a cantidade (integridade), a calidade (exactitude e fiabilidade) e o tempo (dispoñibilidade) da produción. Os auditores de TI poden sinalar as ineficiencias se hai duplicación dos procesos, demora indebida de calquera proceso, controis innecesarios incorporados no sistema, etc.

O exame da eficacia en relación á implementación dos sistemas de TI, implicaría establecer se cumpriu os seus obxectivos, o que entre outras cousas, implica cumprir coas metas e obxectivos xerais da entidade. A non consecución dos obxectivos da entidade na utilización do sistema de TI podería indicar a utilización ineficaz do mesmo.

A auditoría operativa tamén contribúe á rendición de contas e a transparencia. Debe centrarse nas áreas nas que pode achegar un valor engadido para os cidadáns e que teñen o maior potencial de mellora. Ademais, proporciona incentivos construtivos para os responsables de tomar as medidas apropiadas. A implementación de TI, nas organizacións públicas, é a miúdo unha iniciativa nova. Consecuentemente, o enfoque da auditoría operativa de TI que promova o bo goberno na utilización de TI debe ser un dos elementos esenciais do enfoque de auditoría TI. As deficiencias descubertas deben sinalarse dunha maneira que conduza a melloras no sistema, en lugar de matar a iniciativa.

14.7 Os auditores de TI poden ser chamados a prestar asistencia nas auditorías no uso de CAATs. As condicións do encargo, en tal caso, serán útiles para decidir se a intervención constituiría unha auditoría de TI. O uso de CAAT só para levar a cabo a análise de datos non é unha auditoría de TI onde non leva a cabo a avaliación dun sistema TI.

15. Alcance da auditoría de TI

Requirimento:

Os auditores de TI deben determinar o alcance da auditoría durante a etapa de planificación para asegurar o logro dos obxectivos da auditoría.

Explicación:

15.1 Unha vez decididos os obxectivos das auditorías de TI, os auditores de TI tamén deben decidir sobre o alcance da auditoría. Xeralmente, os dous pasos realízanse de forma simultánea. O alcance da auditoría de TI implicará decidir a extensión do exame de auditoría, en termos de cobertura dos sistemas de TI e as súas funcionalidades, os procesos de TI a auditar, a localización dos sistemas de TI a cubrir, o período de tempo a cubrir e, ademais, o tipo de auditoría (auditoría financeira / de cumprimento / de operativa). Será, basicamente, o establecemento ou a definición dos límites da auditoría.

15.2 Os sistemas de TI apoian as funcións de xestión nunha entidade e polo xeral implican procesos de TI específicos, como a introdución de datos no sistema, a solicitude de información e a xeración de informes. A maioría dos sistemas de TI atópanse nunha localización específica xunto co equipo de rede asociado. A seguridade da localización física e os equipos que conteña podería ser cuberta na auditoría de TI.

15.3 O auditor debe seleccionar o período de tempo para a análise de auditoría (é dicir, examinar a información de 1 ano, 3 anos, ou máis, etc.) que permita aos auditores de TI obter conclusións adecuadas nas auditorías realizadas. Ao auditar o sistema de TI, o período de tempo a cubrir pode ser definido a partir dos requisitos da auditoría correspondente.

15.4 O alcance da auditoría tamén implicará centrarse en dominios específicos do sistema de TI que serían de relevancia para o obxectivo da auditoría de TI. Os dominios de TI típicos son o bo goberno de TI, desenvolvemento e adquisición, operacións de TI, outsourcing, seguridade de SE, plan de continuidade de negocio e plan de recuperación de desastres, e controis de aplicación[23]. Estes dominios serían xeralmente suficientes para calquera sistema de TI. Con todo, como o campo de TI está en constante cambio, os auditores de TI non deben excluír a posibilidade de incorporar novas áreas dentro do alcance das súas auditorías, se se consideran pertinentes[24]. Unha auditoría de TI integral requiriría o exame de todos os dominios de TI.

15.5 O alcance da auditoría depende do perfil de risco do sistema de TI que está a ser auditado, así como dos recursos dispoñibles. Se os riscos son maiores, o alcance poida que teña que ser estreito, pero extenso na cobertura dentro do alcance da auditoría de TI.

16. Capacidades dunha EFS para levar a cabo as auditorías de TI

Requirimento:

A EFS deberá ter a capacidade adecuada para levar a cabo a auditoría de TI.

A EFS deberá desenvolver a capacidade adecuada, se esta non está dispoñible, antes de comezar unha auditoría de TI.

Explicación:

16.1 A función básica de todas as EFS é auditar e poida que xa posúan as capacidades de auditoría. Con todo, a auditoría de TI require capacidades específicas. Algunhas das capacidades que un equipo de auditoría de TI debe posuír colectivamente son:

i. Persoal con experiencia e coñecementos en TI;

ii. Comprensión das regras e normas existentes, ou a contorna, no que o sistema de TI está a funcionar;

iii. Comprensión das normas/directrices de auditoría de TI aplicables á EFS; iv. Comprensión das técnicas de TI para obter evidencia de auditoría de sistemas automatizados;

v. Comprensión das ferramentas de auditoría de TI adecuadas para recoller, analizar, reproducir os resultados de dito análise ou volver a realizar as funcións auditadas;

vi. Adecuada infraestrutura de TI para capturar e reter a evidencia de auditoría;

vii. Dispoñibilidade de ferramentas de auditoría TI adecuadas para analizar os datos obtidos.

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

[24] Capítulo 9, temas de interese adicionais, WGITA-IDI Manual sobre Auditorías de Tecnoloxías da Información para as Entidades Fiscalizadoras Superiores.

17. Asignación de recursos

Requirimento:

A EFS deberá identificar e asignar recursos adecuados e competentes para levar a cabo a auditoría de TI.

Explicación:

17.1 As EFS teñen moitas opcións diferentes para asignar recursos á auditoría de TI.

17.2 O enfoque máis común é ter un grupo central con especialistas en TI ou expertos que axudan a outros no organismo a levar a cabo as auditorías de TI. A EFS debe ser capaz de aproveitar as habilidades duns poucos para levar a cabo as auditorías de TI, en caso que estean recentemente empezando por este camiño.

17.3 Outra opción é colocar especialistas de TI en cada un dos equipos dentro da EFS. Con todo, se cada equipo leva a cabo só unhas poucas auditorías de TI, entón isto podería ser un uso ineficiente do especialista en TI. A medida que o número de auditorías de TI aumenta, as EFS tenden a establecer unha función ou grupo de auditoría de TI especializado. Este grupo é, entón, o responsable de levar a cabo todas as auditorías de TI que a EFS realiza.

17.4 O grupo de TI pode interactuar con outros equipos na EFS que teñan un acervo de coñecemento da entidade, isto permite que o equipo de auditoría de TI obteña rapidamente o coñecemento da actividade da entidade e relacione os procesos de xestión cos sistemas TI que os soportan, a fin de facilitar a auditoría de TI.

18. Contratación de recursos externos

Requirimento:

A EFS pode considerar a contratación de recursos externos para levar a cabo a auditoría de TI, se a capacidade non está dispoñible internamente.

Explicación:

18.1 A EFS pode decidir utilizar recursos externos para levar a cabo a auditoría de TI ou externalizar a auditoría de TI contratando a expertos, se ten recursos limitados. Tales recursos serán principalmente consultores externos que sexan expertos en técnicas e ferramentas de auditoría de TI, incluíndo bases de datos, programación e outras áreas relevantes para a auditoría de TI. Os recursos tamén inclúen calquera infraestrutura de TI necesaria na EFS para realizar a auditoría. Polo xeral, son os mesmos que se utilizan para levar a cabo calquera outra auditoría, con todo, a auditoría de TI podería requirir ferramentas específicas de análises, conversión e almacenamento de datos.

18.2 O traballo dos recursos externos, cando se externalizaron, debe ser controlado adecuadamente pola EFS, a través dun contrato escrito ou un acordo de nivel de servizo. O traballo e os produtos finais entregados á EFS deben seguir os procesos e normas existentes adoptadas pola EFS. Isto significa que a EFS en calquera caso requirirá de persoal interno cualificado e informado para supervisar o traballo.

19. Vinculación coa entidade auditada

Requirimento:

A EFS deberá vincularse coa entidade auditada antes do inicio da auditoría.

Explicación:

19.1 Como en calquera auditoría a entidade auditada deberá estar familiarizada co alcance, os obxectivos e os criterios de avaliación da auditoría, que deben ser discutidos con ela cando sexa necesario. A EFS pode, se fose necesario, escribir a carta de compromiso á entidade auditada, onde tamén poderá establecer os termos de ditos compromisos.

19.2 En concreto para a auditoría de TI, a EFS debe asegurarse de que se busque a debida cooperación e o apoio da entidade auditada na realización da auditoría, incluíndo o acceso aos rexistros e a información, e as disposicións adoptadas para obter datos electrónicos no formato necesario para permitir a súa análise.

20. Evidencia de auditoría

Requirimento:

A EFS asegurarase de que as evidencias de auditoría sexan suficientes, fiables e precisas para soster as observacións da auditoría.

As evidencias de auditoría estarán dispoñibles para recrear e revisar o proceso de auditoría posterior ao peche da auditoría.

Explicación:

20.1 A evidencia de auditoría é a recompilación de datos, rexistros, documentos e información obtida polos auditores de TI para fundamentar as súas observacións á parte interesada(s) no momento preciso (no momento da auditoría ou posteriormente), de maneira suficiente, fiable e exacta.

20.2 Como tal, a evidencia debe ter as características de suficiencia, fiabilidade e exactitude/precisión de acordo coas normas de garantía de calidade internas da EFS.

20.3 A evidencia nunha auditoría de TI debe ser adecuadamente recollida e almacenada de forma que estea dispoñible no futuro sen que os datos sexan alterados. Os auditores de TI deben asegurarse de que a evidencia teña selo de tempo[25] nos casos en que exista risco de que a evidencia poida ser alterada.

20.4 As auditorías de TI presentan diferentes e específicas maneiras de identificar, recoller, almacenar e conservar evidencia. A evidencia pode obterse das probas específicas realizadas sobre as mostras baixo observación de auditoría. Os auditores de TI poderían levar a cabo as probas en todas as transaccións ou nunha mostra, segundo sexa necesario, pero os datos electrónicos sempre se poden probar fronte a un criterio na súa totalidade. Con todo, a verificación das excepcións pode levarse a cabo de forma selectiva, se as hai en gran número. A mostra de auditoría pode ser elixida aleatoriamente ou de maneira sistemática. Poden utilizarse mostraxes de unidades monetarias ou tamén é posible que a mostra sexa seleccionada con base a unha decisión razoada dos auditores de TI.

20.5 As técnicas e ferramentas específicas para colleitar evidencia de auditoría nas auditorías de TI discútense máis adiante na sección D.

21. Execución da auditoría – Recompilación de evidencia de auditoría

Requirimento:

O auditor de TI debe reunir evidencia de auditoría adecuada e suficiente, e analizar a mesma para asegurar que os obxectivos da auditoría sexan abordados adecuadamente.

Explicación:

21.1 Avaliación preliminar dos controis de TI

Os auditores de TI deben levar a cabo unha avaliación preliminar dos controis de TI no sistema obxecto da auditoría, para obter a seguridade de que os controis de TI existentes (controis de TI xerais e controis de aplicación) son fiables e funcionan baixo un marco de gobernanza de TI adecuado. A avaliación dos controis a este nivel incluiría:

a) Avaliar que os mecanismos adecuados de gobernanza de TI estean establecidos e funcionando;

b) Avaliar que os obxectivos de TI estean aliñados cos obxectivos de negocio;

c) Avaliar que os mecanismos adecuados estean establecidos para:

i. A xestión efectiva de proxectos de TI ;

ii. A adquisición e desenvolvemento dunha solución de TI (que abarca aplicacións de TI, hardware, software, persoal, rede, solucións de servizos, etc.);

iii. O funcionamento dos sistemas de TI;

[25] Un selo de tempo é un dato que se engade á información (electrónica, papel, vídeo, etc.) para etiquetar o momento en que se xerou, recompilou ou editou a información. Os selos de tempo poden ser tan detallados como sexa necesario (día, data, horas, minutos, segundos, milisegundos, etc.) para a información.

iv. Garantir a seguridade da información;

v. Garantir a continuidade do negocio e a recuperación de desastres;

vi. Garantir unha adecuada xestión do cambio;

vii. Garantir a entrega do servizo e retroalimentación;

viii. Asegurar o cumprimento de normas, regulamentos e procedementos establecidos a través do monitoreo e control.

Os anteriores, salvo o punto (vii), comprenden controis xerais de TI que non son específicos para calquera fluxo de operación individual ou aplicación, senón que se relacionan coa infraestrutura global de TI da entidade, incluíndo as políticas, procedementos e prácticas de traballo relacionadas con TI, así como os controis das operacións do centro de datos (políticas e normas de TI), adquisición e mantemento de software de sistemas, seguridade de acceso (físico e lóxico), segregación de funcións, continuidade de negocio e controis de recuperación de desastres, e desenvolvemento e mantemento de aplicacións.

Complementando a avaliación dos controis xerais de TI estaría a comprensión dos procesos de negocio, o mapeo dos procesos de negocio no sistema de TI e os controis de aplicación de TI asociados.

As excepcións identificadas despois dunha avaliación preliminar, conducirían ás decisións sobre as probas substantivas do sistema de TI e os seus controis.

21.2 Probas substantivas

As probas substantivas consideran probas detalladas dos controis de TI, como na avaliación preliminar, empregando diversas técnicas e ferramentas para a investigación, extracción e análise de datos. As probas substantivas están deseñadas para corroborar as afirmacións de acordo cos obxectivos de auditoría. As probas teñen que ser deseñadas especificamente, utilizando unha ou máis das técnicas[26] descritas na sección D.

22. Supervisión e revisión

Requirimento:

A EFS deberá garantir que as auditorías de TI sexan supervisadas e revisadas periodicamente.

Explicación:

22.1 O traballo do persoal de auditoría debe ser adecuadamente supervisado durante a auditoría e o traballo documentado debe ser revisado polo líder do equipo de auditoría de TI (Elemento 5 - Desempeño de auditorías e outros traballos' - ISSAI 40). O membro senior do equipo debe ter a competencia necesaria para proporcionar orientación e asumir o rol de mentor e guía durante a realización da auditoría.

23. Casos de fraude, corrupción e outras irregularidades

Requirimento:

As EFS e os auditores de TI deben identificar e valorar os riscos e fraudes relevantes para os obxectivos das auditorías de TI.

A EFS deberá tomar as accións que correspondan, segundo o establecido nas leis aplicables, para tratar os casos de fraude, corrupción e outras irregularidades.

Explicación:

23.1 Na realización da auditoría, os auditores de TI poden atoparse con casos de fraude, corrupción e irregularidades asociadas. Os requisitos para formular unha denuncia de fraude poden estar contidas no mandato de auditoría ou en normas xerais, como leis ou regulamentos, e pode ser necesario que o auditor comunique estas cuestións a terceiros alleos á entidade auditada, tales como as autoridades regulatorias ou outras competentes. En tal situación, a EFS debe tomar as medidas que fosen

[26] As técnicas poden ser utilizadas nas probas de cumprimento e substantivas. O auditor de TI pode elixir unha ou máis destas técnicas, mentres realiza calquera das dúas avaliacións.

procedentes, nos termos definidos pola norma aplicable.

23.2 Na realización da auditoría, os auditores de TI deben manter unha actitude de escepticismo profesional e estar alertas á posibilidade de fraude en todo o proceso de auditoría.

24. Limitacións

Requirimento:

A EFS debe identificar, indicar e comunicar aos niveis apropiados as limitacións en todas as etapas da auditoría.

Explicación:

24.1 As limitacións á auditoría de TI deben ser sinaladas en cada etapa de auditoría de TI aos niveis apropiados, a través dunha comunicación documentada e adecuada.

24.2 As limitacións á auditoría de TI deben sinalarse no informe.

24.3 As limitacións típicas poden ser un acceso inadecuado aos datos e información, a falta de documentación adecuada do proceso de informatización, o que leva aos auditores de TI a idear os seus propios métodos de investigación e análise para obter as conclusións. Calquera outra limitación que enfronten os auditores de TI, debe sinalarse adecuadamente no informe.

25. Seguimento

Requirimento:

A EFS debe facer o seguimento dos asuntos relevantes incluídos nos informes de auditoría.

Explicación:

25.1 As EFS teñen un papel no seguimento das accións tomadas polo auditado, en resposta ás cuestións expostas nun informe de auditoría. O seguimento céntrase en se a entidade auditada abordou adecuadamente as cuestións expostas, incluída calquera implicación máis ampla. Por exemplo, se o mesmo sistema de TI é utilizado por moitas organizacións públicas, unha acción insuficiente ou insatisfactoria por parte da entidade auditada pode requirir un novo informe da EFS.

D. TÉCNICAS E FERRAMENTAS DE AUDITORÍA DE TI

Requirimento:

A EFS deberá implementar técnicas de auditoría de TI adecuadas, de conformidade coa natureza do traballo de auditoría e os requisitos dos obxectivos da auditoría.

Explicación:

26. Identificación das técnicas específicas de auditoría de TI

26.1 As técnicas de auditoría de TI relaciónanse coa implementación de métodos e procedementos mediante os cales se poida estudar o ambiente de contorna nun sistema de TI, pódese obter evidencia e facer a análise necesaria para obter seguridade sobre a idoneidade dos controis.

27. Técnicas de planificación

27.1 Durante a planificación dunha auditoría dun sistema de TI, o auditor ten que entender primeiro como unha aplicación en particular soporta un proceso de negocio da entidade auditada. Para este propósito, necesítase obter información básica sobre a forma en que a funcionalidade de negocio flúe a través do sistema. As técnicas de auditoría tradicionais como o estudo de documentos, as entrevistas co persoal clave - tanto os responsables dos procesos de xestión, como as persoas na organización de TI - e a observación dos procedementos, son útiles para obter unha boa comprensión de como o sistema soporta a actividade da entidade. O estudo das políticas e procedementos de TI, os manuais de usuario de aplicación específica, a documentación sobre contratos de externalización de TI, os documentos de deseño funcionais, os manuais de referencia técnicos subministrados polo provedor e a lista de informes (estándares e personalizados), axudan a comprender a contorna no que opera o sistema e a identificación dos riscos de negocio derivados das fallas de control.

27.2 Durante as etapas de planificación anual e de equipo das auditorías de TI, son abordadas as avaliacións de risco dos sistemas de TI que están a ser desenvolvidos ou están en uso en varias entidades auditadas. Estas poden ser obxectivamente levadas a cabo mediante a aplicación das técnicas que se describen na sección de planificación deste documento estándar.

28. Técnicas de execución de auditoría

28.1 A elección das técnicas a utilizar é crucial na realización das probas de cumprimento (probas de controis) e substantivas. As probas substantivas deben estar deseñadas para corroborar as afirmacións de acordo cos obxectivos de auditoría. As probas teñen que ser especificamente deseñadas, usando unha ou máis de técnicas[27], tales como entrevista, cuestionario, observación, probas paso a paso, diagramas de fluxo, captura e análise de datos, verificación, re-cálculo, reprocesamento, confirmación de terceiros, etc.

28.2 Para unha avaliación da idoneidade dos controis xerais de informática - que abarcan os dominios de goberno de TI, adquisición e desenvolvemento de sistemas, operacións de TI, seguridade da información e planificación da continuidade do negocio - as técnicas utilizadas son similares ás usadas noutros tipos de auditoría.

28.3 As técnicas de auditoría específicas para a auditoría de TI son utilizadas principalmente para a avaliación dos controis da aplicación de TI. Durante a proba dos controis da aplicación, o auditor necesita:

I. Identificar os compoñentes significativos da aplicación e o fluxo de información a través do sistema, e obter unha comprensión detallada da aplicación mediante a revisión da documentación dispoñible e a entrevista do persoal adecuado.

II. Entender os riscos dos controis da aplicación e o seu impacto mediante a revisión da criticidad dos procesos de xestión afectados.

III. Desenvolver unha estratexia de probas para identificar as fortalezas e debilidades de control e a avaliación do impacto destas.

28.4 Para unha mellor comprensión do sistema obxecto da auditoría, incluíndo os seus puntos de control claves e o desenvolvemento da estratexia de probas a ser adoptada, é sempre útil examinar a documentación relacionada, tales como as especificacións de deseño funcional, a documentación de xestión de cambio desde o primeiro despregamento ou a última auditoría, manuais de usuario, manuais de referencia técnicos subministrados polo provedor, etc.

28.5 A estratexia de probas tamén dependerá de factores tales como activos en risco, o tempo de existencia da aplicación de xestión, a calidade dos controis internos, a sensibilidade das operacións, os cambios significativos de procesos de xestión que resultan en cambios na aplicación e os resultados das auditorías anteriores, se os hai.

28.6 Para avaliar a segregación de funcións e a autorización de entradas, sería importante revisar as descricións de postos de traballo, relacionalas cos privilexios asignados no sistema, revisar os procedementos de autorización e confirmar a existencia de rexistros de accións (logs) das contas de usuario que teñen privilexios de administrador. Este rexistro de accións require testearse para evidenciar o control xerencial.

28.7 As entidades auditadas terán a súa propia combinación de hardware, sistema operativo, sistemas de xestión de bases de datos, aplicacións de software, software de rede, etc. Os auditores de TI deben ser capaces de reunir información destas fontes para levar a cabo a análise requirida das aplicacións de TI. A comprensión do sistema de TI e da base de datos da organización, como tamén os procesos de xestión involucrados, a súa criticidade para a organización, os protocolos involucrados, etc., é un paso esencial para a extracción de datos. As probas substantivas da idoneidade dos controis de aplicación implica:

a. Extraer datos de xestión relevantes da entidade;

b. Transformar e cargar os datos nunha ferramenta;

c. Realizar unha análise de datos;

[27] Estas técnicas poden ser utilizadas nas probas preliminares e substantivas. As aplicacións de moitas das técnicas están dispoñibles no Manual WGITA IDI sobre Auditorías de TI para Entidades Fiscalizadoras Superiores

d. Validar os resultados das probas;

e. Sacar conclusións de auditoría.

Estes procedementos pódense levar a cabo polos auditores de TI, coa axuda das técnicas descritas no anexo A.

29. Elección dun adecuado sistema de preservación de información

29.1 Os auditores de TI deben garantir a conservación dos resultados e da evidencia da auditoría para axustarse aos requisitos de fiabilidade, integridade, suficiencia e exactitude. Así mesmo, é importante para os auditores de TI asegurar que o proceso de auditoría tamén se conserve para permitir a verificación posterior dos procedementos de análises de auditoría. Isto implica técnicas de documentación adecuadas, que se tratarán posteriormente.

29.2 Durante o requirimento de datos, e na medida do posible, pódese usar unha carta de acompañamento. Se isto non é posible, débense xerar documentos internos onde se anote a información importante, como a data en que foron entregados os datos, de que arquivo creouse o envorcado de datos e[28] se os datos foron provistos desde a contorna de produción ou dalgunha outra contorna, etc. A evidencia electrónica xerada e utilizada para a presentación de informes de auditoría debe estar relacionada con ditos documentos.

29.3 Os auditores de TI deberían decidir sobre a conveniencia da utilización dunha ou máis das técnicas anteriores e asegurarse por si mesmos da integridade e utilidade da técnica. O uso de calquera das técnicas anteriores non debería afectar a integridade do sistema de aplicación e os seus datos na entidade auditada.

30. Ferramentas de auditoría de TI

Requirimento:

A EFS utilizará ferramentas de auditoría de TI acordes coa valoración do risco na auditoría, conxuntamente coa capacidade e os recursos dispoñibles na EFS.

Explicación:

30.1 A auditoría de TI require un bo coñecemento acerca dos procesos e técnicas, xunto con competencia no uso das ferramentas de auditoría de TI, xa que estas auditorías, pola súa propia natureza, ocúpanse de información que se almacena e procésase en forma electrónica, de modo que a pista de auditoría non é visible.

30.2 **As técnicas de auditoría asistidas por computador (CAAT)** son ferramentas de TI que axudan a un auditor na realización de diversas probas automatizadas para avaliar un sistema de TI ou de datos. Estes son moi útiles naqueles casos en que un volume importante de datos dunha entidade auditada está dispoñible en formato electrónico. As CAAT son útiles para a proba dos controis e as probas substantivas na auditoría financeira, a auditoría de cumprimento e a auditoría operativa. O uso das CAAT e a extensión do seu uso, está determinado por varios factores durante as etapas de planificación e execución da auditoría.

30.3 Utilidade das CAAT:

As CAAT son moi útiles para levar a cabo as actividades de auditoría de TI, tales como a análise de rexistro de usuario, os informes de excepcións, a totalización, a comparación de arquivos, a estratificación, a mostraxe, as procuras de duplicados, a detección de faltantes ou brechas, a antigüidade, os cálculos de campos virtuais, etc. (estes elabóranse na sección sobre técnicas de auditoría de TI). O uso das CAAT outorga moitas vantaxes en comparación co exame manual. Algunhas destas son:

a. As probas substantivas e a análise de grandes volumes de datos pódese facer nun curto espazo de tempo e con menos esforzo;

b. As probas pódense repetir facilmente en diferentes arquivos/datos;

[28] O envorcado de datos defínese como unha gran cantidade de datos transferidos desde un sistema ou ubicación a outra

c. As probas flexibles e complexas pódense facer cun cambio nos parámetros;

d. Documentación automatizada de probas e resultados de auditoría;

e. Implementación máis eficiente dos recursos de auditoría.

30.4 Elección de CAAT cando se realiza unha auditoría de TI: O uso de CAAT ten custos asociados en termos de licenzas de software, compatibilidade de hardware e a existencia de persoal de auditoría cualificado. Polo tanto, algúns factores importantes que deben considerarse ao decidir sobre o uso de CAAT na auditoría de TI son os seguintes:

a. ¿Proporciona un valor adicional á auditoría o uso de CAAT?

b. ¿Van ser repetidas as probas noutras/futuras auditorías da mesma entidade auditada ou outras entidades auditadas cuxa actividade e operacións sexan similares?

c. ¿Procésanse as operacións en liña e/ou en tempo real?

d. ¿O uso doutras técnicas de auditoría implicaría maiores custos e tempo extra?

30.5 Algúns exemplos destacados de CAAT son:

- Un software de auditoría de propósito xeral é desenvolvido para satisfacer as necesidades específicas dos auditores e contén as probas habituais que levan a cabo os auditores de TI como parte da auditoría. Inclúen funcións comúns como a extracción de datos, resumo, antigüidade, estratificación, procura de duplicados, etc;

- A linguaxe de consulta estruturadao (SQL) utilízase para definir e manipular datos en sistemas de xestión de bases de datos relacionais (RDBMS);

- As follas de cálculo son tamén CAATs útiles e pódense utilizar para executar consultas sinxelas, como a extracción de datos que cumpren criterios predeterminados, clasificación, totalización, etc;

- As ferramentas de minería de datos axudan a descubrir patróns en grandes conxuntos de datos , a extraer información con eles e a transformalos nunha estrutura comprensible para o seu uso a través da visualización de datos.

- Software de auditoría específico para o sector industrial desenvólvense co obxectivo de proporcionar funcionalidades para atender as tarefas de auditoría máis comúns asociadas con industrias específicas, é dicir, que capturan a lóxica específica da industria para crear consultas de auditoría, etc. Atópanse nas industrias con procesos de negocio ben documentados e establecidos, tales como a banca, manufactura, petróleo e gas, transporte marítimo, etc.

- O software de utilidades realiza funcións deseñadas para axudar a analizar, configurar, optimizar ou manter a infraestrutura de TIC. Os principais exemplos relacionados coa auditoría de TI son, entre outros, utilidades para o control de revisións, depuradores, analizadores de espazo en disco, administradores de arquivos, utilidades de rede e perfiladores de sistemas

- Algúns sistemas ben desenvolvidos incorporaron módulos de auditoría (software de auditoría especializado) que xeran informes estandarizados, como tamén personalizados. Estes veñen como funcionalidades integradas de aplicacións de planificación de recursos empresariais (ERP). Ademais, hai software comercial que dá aos auditores de TI acceso de só lectura a datos de ERP a través de aplicacións baseadas en interfaces.

30.6 Co fin de utilizar CAAT para auditar unha área particular, o auditor debería planificar en detalle. É importante entender e obter información/detalles, entre outros, sobre as relacións entre táboas/arquivos, dicionario/triggers (detonantes) de base de datos, esquema de datos, controis totais, tamaño/formato de datos e documentación do sistema, antes de comezar unha auditoría na que se utilice CAAT.

E. PRESENTACIÓN DE INFORMES

Requirimento:

Os informes de auditoría de TI deberán reflectir os achados do proceso de auditoría de TI, en función da materialidade de tales achados en relación aos obxectivos da auditoría.

O informe de auditoría de TI deberá ser completo, equilibrado, convincente, oportuno e fácil de ler.

Explicación:

31. Requirimentos de presentación de informes dunha auditoría de TI

31.1 Dado que a auditoría de TI pode formar parte dunha auditoría financeira, operativa, de cumprimento ou dunha combinación destas, os requisitos de presentación de informes dunha auditoría de TI provirán, do mesmo xeito, das ISSAI 100-400 e dependendo da natureza da auditoría que leva a cabo, das ISSAI 1700, 1705 e as ISSAI 1706 no caso da auditoría financeira e as respectivas ISSAI nivel 4 sobre auditoría de cumprimento e auditoría operativa.

31.2 Algunhas consideracións que os auditores de TI deben ter en conta son limitar o uso da xerga técnica, ter en conta a sensibilidade da información que se presenta no informe, por exemplo, contrasinais, nomes de usuarios, ID e información persoal.

32. Contidos e formato do informe de auditoría de TI

32.1 O formato xeral dun informe de auditoría de TI inclúe o seguinte;

a. Os obxectivos da auditoría;

b. O alcance da auditoría;

c. As datas aplicables á cobertura da auditoría;

d. Os criterios da auditoría;

e. A metodoloxía da auditoría;

f. O resumo;

g. Os achados da auditoría;

h. As conclusións da auditoría;

i. As recomendacións da auditoría;

j. Calquera causa(s) e risco(s) asociado, restricións, reservas, limitacións ou preocupacións que o auditor poida ter en relación coa auditoría realizada por el/ela.

32.2 A pesar da natureza técnica dunha auditoría de TI, os auditores de TI deben asegurarse de que o informe sexa totalmente comprensible pola alta dirección, a entidade auditada, as partes interesadas e o público en xeral.

32.3 Os auditores de TI poderán debater o proxecto de informe co xestor do sistema de TI auditado antes da finalización e emisión e incluír a súa resposta aos achados, conclusións e recomendacións no informe final, se correspondese.

32.4 A unidade auditada poderá decidir aceptar o risco de non corrixir unha condición informada debido ao custo, a complexidade da acción correctiva ou outras consideracións. O informe de auditoría de TI debe mencionar este feito ás autoridades responsables, de acordo co seu marco de actuación.

32.5 No caso de que os auditores de TI e a unidade auditada non estean de acordo sobre unha recomendación de auditoría ou comentario en particular, o informe de auditoría pode expor ambas posicións e as razóns do seu desacordo nun apéndice. Como alternativa, as opinións da unidade auditada poden ser presentadas no corpo do informe ou nunha carta de presentación.

32.6 Os auditores de TI poden considerar o posible impacto negativo do informe unha vez que se publiquen os informes das EFS. Polo tanto, se os auditores de TI atopan problemas de seguridade no sistema de TI e informáronos antes de que o sistema informático sexa reparado, a vulnerabilidade do sistema de TI é

exposta ao público antes de ser corrixida. En tal escenario, as EFS poden considerar opcións tales como a presentación de informes despois de que o sistema de TI sexa reparado, ou non informar da vulnerabilidade en detalle, para evitar o efecto adverso do informe.

32.7 O seguimento de calquera auditoría é a culminación de todo o proceso de auditoría de TI. Levarase cabo para asegurar que as deficiencias que se identificaron no curso dunha auditoría de TI, fosen posteriormente abordadas de maneira satisfactoria. Polo xeral, é o resultado dunha valoración de riscos continua que é levada a cabo por unha EFS. Como parte do seguimento dunha auditoría de TI cuxo informe foi presentado, o auditor de TI volve revisar unha auditoría despois dun lapso de tempo razoable para asegurar que se aplicaron todas as recomendacións.

Anexo A - Técnicas de análises de datos

1. Extracción de datos de xestión relevantes da entidade:

Comprender a estrutura de datos mediante a obtención e o estudo dos documentos de definición de datos da entidade auditada. Se a entidade auditada concede acceso de só lectura ao sistema, entón os datos almacenados nas táboas pertinentes para a auditoría, poden ser extraídos mediante a consulta da base de datos se se posúen as habilidades. Pola contra, pódese solicitar á entidade que proporcione unha copia dos datos de orixe pertinentes. Os datos poden ser recibidos en forma dun envorcado de base de datos que conteña un rexistro da estrutura da táboa e/ou os datos dunha base de datos, usualmente en forma dunha lista de comandos SQL. Os auditores de TI poderían ter que crear un ambiente similar (versións compatibles das aplicacións máis comúns de bases de datos, sistemas operativos, hardware, etc.) ao da entidade auditada para importar/analizar os datos da copia dos envorcados de datos extraídos. En moitos casos, isto representa o aspecto máis importante das probas dos controis de aplicación, xa que a correcta extracción de datos senta as bases para o éxito dos procesos posteriores. Tamén pode ser necesario que os auditores de TI convertan os datos dunha forma a outra para facilitar unha mellor lectura e análise.

2. Transformación e carga de datos:

Utilice o software de auditoría/ferramentas de extracción, transformación e carga, para importar datos desde diversas plataformas de base de datos. As ferramentas de análises de datos utilizadas máis comunmente (analizadas na sección sobre ferramentas) permiten a importación de datos desde múltiples bases de datos, ao formato de folla de cálculo orixinal das ferramentas. Estas ferramentas adoitan utilizar un asistente de importación para axudar na importación (interpretación, conversión, formato) de datos para a súa posterior análise. É importante que o auditor realice algúns pre-formateos dos datos de orixe para facer o exercicio de análise máis fácil. Tamén, poderían utilizarse un software de auditoría xeneralizado ou unha utilidade de software específica para avaliar o funcionamento de varias utilidades dos sistemas de TI. O uso de calquera destes ou a súa combinación, dependerá dos obxectivos da auditoría e o alcance a cubrir nas auditorías de TI.

3. Realización da análise de datos

Os pasos principais na análise dos datos de xestión da entidade auditada para obter seguridade sobre a calidade dos controis de aplicación son comúns a calquera forma de análise de datos. As consideracións claves na análise de datos son as seguintes:

- Identificar a finalidade da análise ou proxecto;
- Comprender a mostra(s) en estudo;
- Entender os instrumentos que se utilizan para recompilar datos;
- Ser consciente do deseño e formato dos datos[29]; e
- Establecer un identificador único se se combina ou fusiona, en caso de ser necesario.
- Os auditores de TI necesitan planificar:
  - A relación de preguntas de investigación / obxectivos
  - Os métodos utilizados para responder as preguntas de investigación
  - Os criterios para a avaliación
  - A evidencia
  - A análise
  - A conclusión
- Os procedementos de reestruturación de arquivo (creación de sintaxe, adición de novas variables, se é necesario)

[29] Este sería un dos pasos máis importantes antes da realización da análise de datos. O deseño significaría a comprensión das diferentes bases de datos, táboas incorporadas, patrón de codificación utilizado e relacións entre táboa e bases de datos. A comprensión dos diferentes modelos de base de datos será útil neste sentido.

- Os procedementos de limpeza de datos (p. ex. a eliminación de valores atípicos)

A maioría das análises pódense executar directamente desde un arquivo de datos de traballo. Algunhas análises poden requirir transformacións de datos brutos, subconxuntos ou datos de entrada específicos para cumprir co software de estatística ou as ferramentas que o auditor pode utilizar.

4. Comprensión dos tipos de datos e a representación

A análise de datos realízase xeralmente nunha copia dos datos recibidos da entidade auditada para preservar o orixinal para a súa posterior confirmación e revisión, se fose necesario.

Pódese utilizar un software de auditoría de propósito xeral ou un software de auditoría especializado para levar a cabo a análise da información. Estas ferramentas ofrecen a facilidade de importar e analizar os datos. Tamén se pode facer uso de Linguaxe de Consulta Estruturado (SQL) na análise de datos. Para sistemas complexos, como os sistemas ERP, a información está dispoñible a través de informes específicos. Os auditores de TI deben entender ditos informes e obter informes pertinentes para levar a cabo unha análise apropiada. Os auditores de TI deben ter coidado en asegurar que os datos obtidos sexan fiables, pertinentes, razoables e suficientes. Deben ter, na medida do posible, selo de tempo e estar debidamente revisados pola organización auditada.

En particular, as variables en varios campos de datos poden requirir codificación especial para a representación diferente de datos

- Numérico
- Cadea de caracteres
- Data e hora
- Monetaria

As **técnicas individuais de análises de datos** para examinar a integridade das aplicacións son dependentes, novamente, dos obxectivos da auditoría. Estas técnicas son:

1. **Uso de datos de proba:** A análise con datos de proba faise en situacións nas que se tenta probar a calidade do programa. A premisa é que é posible xeneralizar acerca da fiabilidade xeral dun programa, se é fiable para un conxunto de probas específicas. O uso dos datos de proba implica o *deseño* de datos de proba e a *creación* de datos de proba antes de executar o programa con este tipo de datos. A miúdo, esta técnica impleméntase na etapa de proba da aplicación polo propio desenvolvedor, antes de que unha aplicación ou cambios nela sexan trasladados á produción (é dicir, operación transaccional en curso). Mentres se audita un sistema de TI recentemente implementado, ou procesos de xestión do cambio, o auditor pode revisar os procedementos realizados na fase de proba.

2. **Comparación de código:** Os desenvolvedores utilizan técnicas de comparación de código que implican a comparación do código fonte dun programa ou das modificacións do mesmo, con metodoloxías de deseño estándar para a linguaxe de programación particular, coa intención de descubrir erros, fallas ou brechas de seguridade das convencións de programación. Na súa maioría son ferramentas dos desenvolvedores e non son utilizadas a miúdo polos auditores de TI. Para as mostras de código seleccionadas polos equipos de probas de seguridade independentes, o papel dos auditores sería determinar que se probou a seguridade do código e que os resultados foron documentados e informados, e que as violacións e as vulnerabilidades detectadas foron debidamente saneadas. Con todo, os auditores coas habilidades adecuadas, poden recorrer á comparación de código en relación coa xestión do cambio ou a posta en marcha dun programa de aplicación, se o alcance o permite.

3. **Proba da integridade de datos:** A proba de integridade de datos é un conxunto de probas substantivas que examinan a exactitude, integridade, consistencia e autorización dos datos dispoñibles no sistema. Estas probas indicarán a debilidade nos controis de entrada ou de procesamento. As probas de integridade de datos axudan a identificar a solidez da integridade relacional, mediante a revisión das rutinas de validación que se incorporaron na aplicación, durante o deseño das limitacións das condicións de entrada e as características dos datos, na etapa de definición de táboa do deseño de base de datos.

   Estas probas implican certas **técnicas de análises de datos** que os auditores de TI poden implementar coa axuda de ferramentas de análises comúns ou de software de auditoría xeneralizados.

4. **Mostraxe:** As técnicas de mostraxe son útiles para obter conclusións adecuadas baseadas en controis

estatisticamente suficientes de datos limitados. Hai dous métodos principais de mostraxe utilizados polos auditores de TI. Estes son a mostraxe de atributos e a mostraxe de variables. A mostraxe de atributos utilízase xeralmente en situacións de probas de cumprimento e aborda a presenza ou ausencia do atributo, proporcionando conclusións que se expresan en taxas de incidencia. A mostraxe de variables aplícase xeralmente en situacións de probas substantivas e aborda as características da poboación que varían, facilitando conclusións relacionadas coas desviacións da norma.

Para as validacións da proba e outros controis de entrada nun sistema que trata cunha gran cantidade de datos, o auditor pode atopar útil extraer unha mostra aleatoria de rexistros de transaccións almacenados na base de datos do sistema.

A maioría das aplicacións de análises de datos, incluíndo aplicacións de folla de cálculo e software de auditoría de propósito xeral provén funcións fáciles para seleccionar un elemento particular de datos (campos/ columnas/ tupla) e as celas de datos relacionados, e crean subconxuntos aleatorios dos datos elixidos, mediante o uso de algoritmos baseados en sementes de número aleatorios, ou fórmulas simples.

5. **Resumo e estratificación:** Estas dúas técnicas axudan á elaboración de perfís de datos antes de que se leve a cabo calquera proba dos controis. O resumo de datos axuda a totalizar as transaccións en termos de atributos definidos, isto axuda ao auditor a obter unha comprensión global das transaccións. Por exemplo, totalizar as contas por cobrar por tipos de cliente proporciona unha información útil sobre os morosos de alto valor. Unha función moi útil dispoñible na folla de cálculo e nas ferramentas de auditoría de propósito xeral é a táboa dinámica, axudando na xeración da información resumida desde unha base de datos grande, nun lapso moi curto de tempo.

   A estratificación dos datos prepara unha distribución de frecuencia dos datos en termos de localizacións ou intervalos definidos. Pódelle dar ao auditor información importante acerca da natureza dos datos e tamén pode axudar a identificar as áreas nas que deben realizarse as probas detalladas.

6. **Consultas condicionais**: A técnica de extracción de datos baseada en consultas condicionais é útil para levar a cabo unha serie de controis sobre a calidade dos controis de aplicación que inclúen probas de completitude, de integridade, de mapeo correcto das regras de xestión.

   a. Proba dos controis de entrada: Por exemplo, nun sistema de TI que pode prestar soporte a un determinado programa de educación / benestar financiado polo goberno, é importante crear rexistros de beneficiarios permanentes en forma de táboas de datos mestres na base de datos. Unha proba dos controis de entrada neste caso consiste en extraer unha mostra de rexistros mestres almacenados na táboa mestra e comprobar se a captura de datos para os atributos relacionados (identificadores únicos, nomes, direccións, identificación de direccións) teñen espazos en branco, valores sen sentido, duplicados, etc. Evidencia de calquera destes erros indicaría deficiencias nas descricións de datos durante o deseño da táboa.

   b. Proba de controis de procesamento: Para as probas dos controis de procesamento unha proba substantiva específica pode ser a de pescudar se unha regra de xestión en particular está mapeada correctamente no sistema de TI que se utiliza para facer o procesamento de negocios. Por exemplo, nun sistema utilizado por unha entidade competente en asuntos tributarios, a proba podería consistir en asegurar que as condicións para a concesión de devolución de impostos estean establecidos no sistema. Neste caso, poderíase facer unha extracción de rexistros do conxunto de datos de impostos da mostra cunha condición que simula a regra de xestión de acordo á lei. Calquera resultado deste exercicio de extracción que non estea conforme coa regra, pode indicar un control de procesamento indebido ou a falta de inclusión da regra de xestión. Tal falta de inclusión leva a erros repetidos, os que poderían dar lugar a un impacto significativo nas finanzas da entidade.

   Os auditores de TI necesitan ter un coñecemento detallado das regras de xestión da entidade para deseñar consultas condicionais significativas, a fin de verificar se as regras de xestión están correctamente descritas na aplicación.

7. **Identificación de duplicados:** Unha proba común da integridade de datos relacionales nunha base de datos é examinar a existencia de duplicados, onde o lóxico é que estes non existisen, en función das regras de xestión definidas pola entidade. Por exemplo, nunha base de datos da seguridade social ou impostos, a identidade relevante defínese como única de acordo á lei. A evidencia de duplicados neste campo de datos, indicaría validacións incorrectas respecto das entradas de datos permanentes, dando

lugar a un risco operativo ou financeiro para a entidade auditada. As ferramentas de análises proporcionan unha función simple para detectar claves duplicadas. Estas pódense atopar mesmo en táboas transaccionais, que poderían aumentar o risco de duplicación de pagos.

Os auditores de TI necesitan avaliar a necesidade de tales probas, dependendo do control de aplicación que se está probando dentro do proceso. Por exemplo, se o auditor está a revisar os controis financeiros dentro das aplicacións de procesamento de contas por pagar, as posibilidades de que o número de orde de compra xerado polo sistema sexa duplicado, serían bastante improbables. Con todo, se o auditor necesita facer probas por controis de presentación de facturas duplicadas de provedor (unha entrada externa), que é unha entrada non xerada polo sistema, esta proba pode ser utilizada.

8. **Análise de brechas (ou faltantes ou espazos en branco):** O obxectivo do uso desta técnica consiste en determinar a integridade e detectar se existen brechas nun campo de datos numérico que se espera que teña unha numeración secuencial. En MS Excel esta atópase a través da clasificación de valores en serie no campo de datos en cuestión, engadindo un campo calculado en base á lóxica secuencial e logo filtrando por filas onde se producen excepcións. O software de auditoría xeral utiliza unha función simple de detección de brechas, onde o campo en cuestión debe ser definido para a identificación das brechas. Para utilizar as funcións de duplicado ou de detección de brechas, o auditor non require moita experiencia en consulta.

9. **Traballo con múltiples arquivos:** A base de datos fonte a miúdo contén gran número de táboas mestras e de transaccións. Ao traballar con conxuntos de datos importados, a miúdo é útil engadir xuntos campos particulares nunha táboa de datos, co uso dunha clave de combinación (campo). O software de auditoría xeral permite dita unión de varios arquivos coa axuda da función de "unión". O uso das funcións de combinación ou consultas condicionais en táboas combinadas, axuda ao auditor a avaliar a integridade referencial entre as táboas de datos ou mesmo entre aplicacións de negocios relacionados separadas, que son usadas pola entidade.

   Por exemplo, se unha entidade rexistra posibles provedores nun portal web e utiliza unha aplicación de adquisición separada para rexistrar as ordes de compra, as regras de xestión deben requirir que a base de datos de provedores estea vinculada á base de datos de adquisicións. Unir táboas destas dúas bases de datos separadas, por medio da combinación de nomes de provedores e ID de provedores axudaría a establecer a adecuación da interface entre as dúas aplicacións de negocios relacionados.

Os auditores de TI teñen que aplicar unha combinación destas técnicas para obter unha seguridade razoable sobre os controis de aplicación.