TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA

RESOLUÇÃO N. 245/2017/TCE-RO

Aprova o Manual de Auditoria em TI – Tecnologia da Informação do Tribunal de Contas do Estado de Rondônia.

O PRESIDENTE DO TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA, no uso das atribuições legais que lhe são conferidas pelo art. 3º da Lei Complementar Estadual nº. 154, de 26 de julho de 1996, c/c o art. 4º do Regimento Interno desta Corte de Contas;

CONSIDERANDO a necessidade de otimização e padronização dos ritos processuais no Tribunal de Contas;

CONSIDERANDO os objetivos do Plano Estratégico 2016-2020 do Tribunal de Contas;

RESOLVE:

Art. 1º Aprovar o Manual de Auditoria em TI – Tecnologia da Informação do Tribunal de Contas do Estado de Rondônia.

Art. 2º Determinar ao Secretario Geral de Controle Externo que mantenha a atualização do Manual de Auditoria em TI, sempre que for constatada sua necessidade, observado o procedimento regimental para alteração da legislação do Tribunal de Contas.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

Porto Velho, de 14 de agosto 2017.

(assinado eletronicamente)
EDILSON DE SOUSA SILVA
Conselheiro Presidente

TRIBUNAL DE CONTAS DO ESTAL
Secretaria Geral de Controle Ex

Tribunal de Contas do Estado de Rondônia

Secretaria Geral de Controle Externo

MANUAL DE AUDITORIA DE TECNOLOGIA DA INFORMAÇÃO

TCE/RO

PORTO VELHO, JUNHO 2017

Conselheiro Edilson de Sousa Silva
Presidente

Conselheiro José Euler Potyguara Pereira de Mello
Vice-Presidente

Conselheiro Paulo Curi Neto
Corregedor

Conselheiros
Valdivino Crispim de Souza
Francisco Carvalho da Silva
Wilber Carlos dos Santos Coimbra
Benedito Antônio Alves

Conselheiros-Substitutos
Francisco Júnior Ferreira da Silva
Omar Pires Dias
Erivan Oliveira da Silva

Adilson Moreira de Medeiros
Procurador-Geral

Procuradores
Érika Patrícia Saldanha de Oliveira
Yvonete Fontinelle de Melo
Ernesto Tavares Victoria

Fernando Soares Garcia
Chefe de Gabinete da Presidência

José Luiz do Nascimento
Secretário-Geral de Controle Externo

Juscelino Vieira
Secretário de Gestão Estratégica da Presidência – interino

Joanilce da Silva Bandeira de Oliveira
Secretária-Geral de Administração

Marcelo de Araújo Rech
Secretário Estratégico de Tecnologia da Informação e Comunicação

Ivaldo Ferreira Viana
Controlador Interno

SUMÁRIO

1. INTRODUÇÃO

Este documento tem como propósito definir os procedimentos básicos para as atividades de Auditoria de Tecnologia da Informação no âmbito do TCE-RO.

Em virtude da vasta experiência e ampla divulgação de informações e estudos nesta área pelo Tribunal de Contas da União (TCU), os quais têm sido referência para estruturação desta área no âmbito de outros Tribunais de Contas do País, optou-se por seguir o modelo e método de trabalho do TCU. Outros TC´s que serviram de referência são os de Pernambuco, Ceará e Rio Grande do Sul.

2. CONCEITOS

A norma ABNT NBR ISO/IEC 38500/2009 define a Tecnologia da Informação (TI) como:

> Os recursos necessários para adquirir, processar, armazenar e disseminar informações. Este termo também inclui "Tecnologia da Comunicação" (TC) e o termo composto de "Tecnologia da Informação e Comunicação" (TIC).

A norma também define quais são esses recursos:

> Pessoas, procedimentos, software, informações, equipamentos, consumíveis, infraestrutura, capital e fundos de operação e tempo.

Nesse contexto, a Auditoria de TI pode ser definida como:

> Processo que busca evidências para certificar-se de que os recursos de Tecnologia da Informação:
>
> - possibilitam que os objetivos do negócio sejam alcançados;

> - são usados com eficiência e em conformidade com as leis e normas aplicáveis; e
> - são adequadamente protegidos para prover informação confiável sempre que requerida às pessoas autorizadas. (PACHECO apud DIAS, 2011).

A Auditoria de TI justifica-se por diversos fatores, dentre os quais está o uso cada vez mais intenso e amplo da TI nas corporações, o que leva a uma dependência crescente, que chega a tornar imprescindível dispor de recursos de TI para a condução dos negócios. Além disso, a informação é um recurso estratégico, que exige cuidados especiais nos procedimentos de aquisição, de manipulação e de armazenamento. Outro ponto que exige atenção é o incremento da interconectividade, que induz maior vulnerabilidade a ameaças externas.

Do ponto de vista organizacional, observa-se um número cada vez maior de sistemas informatizados, cuja complexidade e interconectividade exigem um nível de esforço crescente no seu desenvolvimento e operação. Isso também se reflete na maneira como as empresas conduzem seus negócios, ocasionando mudanças organizacionais e estratégicas. A dependência dos sistemas informatizados também faz com que eventuais erros sejam potencializados, podendo ocasionar danos de grandes proporções. Nesse contexto, torna-se necessária a incorporação de mecanismos de controle cada vez mais poderosos.

Essa mudança no contexto organizacional gera impactos na forma como os entes fiscalizadores exercem suas competências. Torna-se necessária a adaptação dos trabalhos de auditoria, já que o auditor precisa conviver com novos conceitos e metodologias de trabalho. Isso decorre do fato de que grande parte dos controles internos de uma organização está embutida em sistemas informatizados, de onde provêm as informações que servirão de evidência para os achados de auditoria. Assim, é necessário que os entes fiscalizadores estejam preparados para o desafio de auditar uma Administração Pública cada vez mais informatizada, sujeita a maiores riscos e com um sistema de controle interno mais complexo, e frágil sob muitos aspectos. Nesse contexto, uma auditoria de conformidade ou operacional frequentemente requer considerações sobre os controles gerais de TI e, a depender dos objetivos almejados, uma avaliação dos dados.

Importante também observar-se a distinção entre Auditoria de TI e o uso da TI em Auditoria, o que é um conceito de suma importância para a área de Auditoria. A Auditoria de TI é uma função, uma especialidade da Auditoria, assim como a Auditoria Ambiental, a

Auditoria de Obras e a Auditoria de Gestão. Já a TI, através de técnicas e ferramentas, pode e deve apoiar os trabalhos de auditoria, tais como:

a) automação de processos (Planejamento, Execução, Relatório, Monitoramento);

b) gerenciamento da auditoria (p. ex. usar o MS-Project);

c) documentação (p. ex. MS-WORD, Ferramenta Case);

d) ferramenta para comunicação (p. ex. e-mail);

e) base de referências e pesquisas (p. ex. Internet, Intranet, BLM, Sistemas Corporativos, etc);

f) apresentação de auditoria (p. ex. PowerPoint);

g) ferramentas de análise e manipulação de dados (p. ex. ACL, Idea, Access, Excel).

No escopo deste manual, consideram-se seis abordagens de Auditoria de TI: Auditoria de Contratação de TI, Auditoria de Segurança da Informação, Auditoria de Sistemas, Auditoria de Governança de TI, Auditoria de Dados e Auditoria de Políticas e Programas de Governo na área de TI.

Cada uma dessas abordagens observa a área de TI da organização auditada sob um ponto de vista distinto. As abordagens são, portanto, complementares, existindo áreas de intersecção entre elas. Isso ocorre em virtude dos princípios que guiam cada uma dessas abordagens se encontrarem correlacionados dentro de uma estrutura de governança de TI.

A Figura 1 apresenta as principais abordagens de Auditoria de TI, mostrando as áreas de intersecção entre elas.

Abordagens de Auditoria de TI

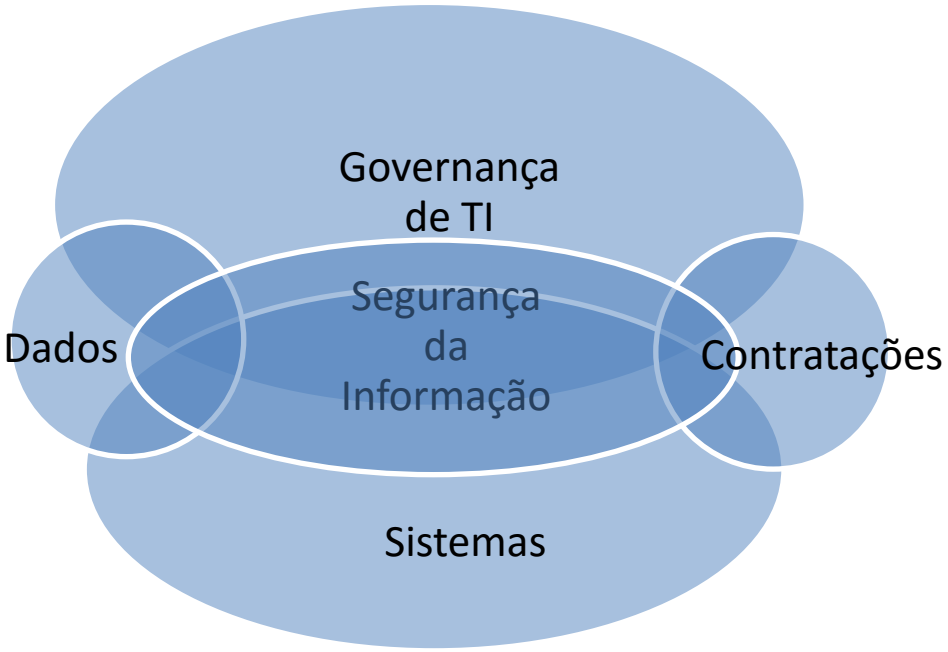


Figura 1- Abordagens de ATI

As Auditorias de TI, dependendo da abordagem, podem mesclar aspectos de auditoria de conformidade e de operacional. Nesse sentido, as atividades de Auditoria de TI serão conduzidas dentro do processo de auditoria ordinária tradicional mas, excepcionalmente, também poderão ser conduzidas por meio de auditoria operacional.

A seguir serão descritas as abordagens de Tecnologia da Informação mais utilizadas nos órgãos de fiscalização e controle, aspectos conceituais de cada abordagem, os principais aspectos abordados e os principais enquadramentos legais utilizados em nível municipal, estadual e federal.

2.1 Auditoria de Contratação de TI

Certifica que os procedimentos adotados pela organização para aquisição de bens e serviços de TI e gestão dos respectivos contratos são eficazes, eficientes, atendem aos objetivos e necessidades do negócio e obedecem aos dispositivos legais.

Principais aspectos abordados:

Aborda os seguintes aspectos: recursos humanos capacitados na gestão de TI, planejamento da contratação, planejamento da TI alinhado ao Planejamento Institucional, parcelamento de serviços, pagamento por resultados, qualidade do serviço e produto, controle efetivo sobre a execução, análise da viabilidade da contratação, plano de sustentação, termos contratuais, análise de riscos, projeto básico ou termo de referência, modalidades e tipos de licitação, aferição de exequibilidade de propostas, contratação direta, registro de preços, manutenção do equilíbrio econômico-financeiro do contrato, transição contratual.

Principais enquadramentos utilizados:

- Constituição da República Federativa do Brasil de 1988.
- Lei Federal n.º 8.248/91 – Direito de Preferência.
- Lei Federal n.º 8.666/93 – Lei de Licitações.
- Lei Federal n.º 10.520/02 – Pregão.
- Norma Técnica Cobit 4.1 (Control Objectives for Information and Related Technology – é um guia de boas práticas, dirigido para a gestão de tecnologia de informação).
  - Planejar e Organizar (PO).
  - AI5.1 Controle sobre Aquisições.

2.2 Auditoria de Segurança da Informação (SI)

É muito importante zelar pela segurança das informações, estejam elas contidas ou não em sistemas computacionais. Informações são recursos patrimoniais críticos, importantes para qualquer organização, tanto para a concretização de negócios como para a tomada de decisão em questões governamentais, sociais, educativas e econômicas.

Como a sociedade moderna depende de informações para tomar decisões de negócio ou de bem estar social, a segurança dessas informações deve ser preservada.

Informações adulteradas, não disponíveis, ou sob conhecimento de pessoas de má-fé podem comprometer instituições do mercado financeiro, indústrias, bancos, sistemas de telecomunicações, de assistência médica, enfim, podem afetar a sociedade de várias maneiras.

São conceitos básicos da Segurança da Informação:

- ✓ **Informação**: É o resultado do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (pessoa ou máquina) que a recebe. A informação é um ativo econômico e estratégico.
- ✓ **Política Corporativa da Segurança da Informação – PCSI**: É um conjunto de princípios, objetivos e diretrizes que norteiam a gestão da Segurança da Informação de uma instituição. As diretrizes estabelecidas nessa política determinam as linhas mestras a serem seguidas pela organização para que seja assegurada a segurança de suas informações;
- ✓ **Sistema de Gestão de Segurança da Informação – SGSI**: Parte do sistema global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

Principais aspectos abordados:

São aspectos básicos da Segurança da Informação: a autenticidade, a preservação da disponibilidade, a integridade e a confidencialidade da informação.

- ❖ Autenticidade: A garantia da veracidade da fonte de informações. Por meio de autenticação, é possível confirmar a identidade da pessoa ou entidade que presta as informações, isto é, se ela é realmente quem deveria ser.
- ❖ Disponibilidade: Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.
- ❖ Integridade: Propriedade de salvaguarda da exatidão e complude de ativos.
- ❖ Confidencialidade: Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

A Segurança da Informação visa evitar e mitigar eventos ou atitudes indesejáveis que potencialmente removem, desabilitam, danificam ou destroem um sistema, recurso ou serviço de informação. Esses eventos são chamados de incidentes, e constituem-se em quaisquer eventos adversos capazes de explorar fragilidades ou deficiências nas medidas preventivas de segurança de uma organização e causar danos, tais como modificação de dados, indisponibilidades de sistemas de informação, divulgação de informações confidenciais, fraude, perda de credibilidade, possibilidade de processo legal contra a instituição e perda de clientes para a concorrência.

Um incidente pode ser acidental (falhas programação, desastres naturais, erros do usuário, de hardware ou software, erros de mensagem secreta enviada a endereço incorreto) ou deliberado (roubo, espionagem, fraude, sabotagem, invasão de hackers). Pode ser ocasionado por pessoa, coisa ou evento capaz de causar dano a um recurso.

Alguns exemplos de incidentes de segurança da informação são os seguintes: vazamento de informações voluntário ou involuntário, violação de integridade ou comprometimento de consistência de dados, indisponibilidade dos serviços de informática, acesso não autorizado e informações classificadas.

Principais enquadramentos utilizados:

- ABNT NBR ISO/IEC 27002:2005 (código de práticas para gestão da segurança da informação).
- Norma Técnica Cobit 4.1 (Control Objectives for Information and Related Technology – guia de boas práticas, dirigido para a gestão de tecnologia de informação).

2.3 AUDITORIA DE SISTEMAS

Essa abordagem tem por objetivo verificar se os sistemas e aplicativos são apropriados, eficientes, e controlados adequadamente para garantir que a entrada, o processamento e a saída de dados são válidos, confiáveis, oportunos e seguros, em todos os níveis de atividade de um sistema.

A Auditoria de Sistemas é um processo realizado por profissionais capacitados e consiste em revisar e avaliar controles para determinar se um sistema suporta adequadamente um ativo de negócio e atinge os objetivos esperados, mantendo a integridade dos dados, utilizando eficientemente os recursos e cumprindo as regulamentações e leis estabelecidas.

As principais técnicas utilizadas são entrevistas, análise documental e observação direta. Outras técnicas comumente utilizadas são os testes de sistema e análises de código-fonte (programas).

Principais aspectos abordados:

O foco da Auditoria de Sistemas é a avaliação das funcionalidades de um sistema. Isso leva a uma diversidade de situações, pois cada sistema implementa funcionalidades específicas do negócio para o qual foi desenvolvido. É necessário, portanto, conhecimento das regras do negócio suportado pelo sistema e também da legislação relacionada.

Os principais aspectos abordados na Auditoria de Sistemas são: a integridade; a disponibilidade; a confidencialidade; a aderência às normas (conformidade); os controles internos; a entrada, o processamento e a saída de dados; a efetividade; a satisfação dos usuários; e a usabilidade de um sistema de informação em particular.

Principais enquadramentos utilizados:

- Legislação e normativos referentes ao negócio suportado pelo sistema auditado;
- Constituição da República Federativa do Brasil de 1988, art. 37, caput (princípio da eficiência);
- ABNT NBR ISO/IEC 27002:2005 (código de práticas para gestão da segurança da informação):
  - 10.3.2 (aceitação de sistemas);
  - 12.2.1 (validação dos dados de entrada);
  - 12.2.2 (controle do processamento interno) o 12.2.4 (validação dos dados de saída).

2.4 Auditoria de Governança de TI

Avalia se o uso da Tecnologia da Informação é eficaz, eficiente e aceitável dentro da organização.

A Governança Corporativa é o sistema pelo qual as organizações são dirigidas e controladas, envolvendo os relacionamentos entre Acionistas/Cotistas, Conselho de Administração, Diretoria, Auditoria Independente e Conselho Fiscal.

A Governança Corporativa de TI é uma parte do Sistema Governança Corporativa. É o sistema pelo qual o uso atual e futuro da TI é dirigido e controlado. Significa

avaliar e direcionar o uso da TI para dar suporte à organização e monitorar seu uso para realizar os planos. Inclui a estratégia e as políticas de uso da TI dentro da organização.

Principais aspectos abordados:

A Governança de TI aborda aspectos de entrega de valor, gerenciamento de risco, alinhamento estratégico, gestão de recursos e medição de desempenho, sendo os dois primeiros relacionados ao efeito da governança e os três últimos habilitadores ou direcionadores.

Esses aspectos são as áreas foco na Governança de TI, segundo o Cobit:

- Alinhamento estratégico: foca em garantir a ligação entre os planos de negócios e de TI, definindo, mantendo e validando a proposta de valor de TI, alinhando as operações de TI com as operações da organização.
- Entrega de valor: é a execução da proposta de valor de TI através do ciclo de entrega, garantindo que TI entrega os benefícios prometidos previstos na estratégia da organização, concentrando-se em otimizar custos e provendo o valor intrínseco de TI.
- Gestão de recursos: refere-se à melhor utilização possível dos investimentos e o apropriado gerenciamento dos recursos críticos de TI: aplicativos, informações, infraestrutura e pessoas. Questões relevantes referem-se à otimização do conhecimento e infraestrutura.
- Gestão de risco: requer a preocupação com riscos pelos funcionários mais experientes da corporação, um entendimento claro do apetite de risco da empresa e dos requerimentos de conformidade, transparência sobre os riscos significantes para a organização e inserção do gerenciamento de riscos nas atividades da companhia.
- Mensuração de desempenho: acompanha e monitora a implementação da estratégia, término do projeto, uso dos recursos, processo de performance e entrega dos serviços, usando, por exemplo, balanced scorecards que traduzem a estratégia em ações para atingir os objetivos, medidos através de processos contábeis convencionais.

A Governança de TI tem como principais objetivos:

- Alinhar os objetivos da TI com os objetivos estratégicos e a finalidade da organização;

- Assegurar a conformidade da TI com as leis e regulamentos;
- Definir com clareza as responsabilidades e obrigatoriedades;
- Assegurar a continuidade e sustentabilidade do negócio;
- Reduzir os custos da organização;
- Obter uma alocação eficiente de recursos.

Principais enquadramentos utilizados:

- Constituição da República Federativa do Brasil de 1988, art. 37, caput (princípio da eficiência);
- Decreto Estadual sobre política de TIC.
- Norma Técnica Cobit 4.1 (Control Objectives for Information and Related Technology – guia de boas práticas, dirigido para a gestão de tecnologia de informação).

2.5 Auditoria de Dados

Essa abordagem tem por finalidade analisar os dados contidos em meios de armazenamento eletrônico, a fim de certificar-se de que são íntegros, confiáveis e encontram-se em conformidade com as leis que regem o negócio.

A Auditoria de Dados pode ser empregada isoladamente ou de forma complementar com outra abordagem (p.ex., auditoria de sistemas). Nesse aspecto, ela tem características comuns com a Auditoria de Sistemas, como, por exemplo, o fato de exigir a compreensão do negócio, para identificar os riscos e selecionar os dados necessários para responder as questões de auditoria.

As técnicas empregadas são a verificação de bases de dados, utilizando recursos do SGBD ou softwares especializados (p.ex., Audit Control Language – ACL). Permite também o cruzamento de informações com outras bases de dados, a fim de verificar os registros auditados.

Principais aspectos abordados:

Os principais aspectos abordados são a integridade, a confiabilidade e a disponibilidade dos dados relacionados ao negócio suportado pelos sistemas de informação.

- Integridade significa que a informação deve ser exata e completa;
- Confidencialidade significa que a informação deve estar protegida contra o acesso e uso não autorizado;
- Disponibilidade significa que a informação deve estar disponível quando requerida.

Além disso, outro aspecto que também deve ser abordado é se os dados respeitam as regras de negócio e obedecem aos controles definidos pela organização e legislação pertinente.

Principais enquadramentos utilizados:

- Legislação e normativos referentes ao negócio suportado pelo sistema auditado;
- Constituição da República Federativa do Brasil de 1988, art. 37, caput (princípio da eficiência).

2.6 AUDITORIA DE POLÍTICAS E PROGRAMAS DE GOVERNO NA ÁREA DE TI

Avalia se as políticas e programas governamentais relacionados à tecnologia da informação são eficazes, eficientes e efetivos.

Esta abordagem se difere das demais, pois não é aplicada a um órgão ou instituição, mas a políticas e programas gerais de governo.

Principais aspectos abordados:

A Auditoria de Políticas e Programas de Governo na área de TI aborda os aspectos de governança de TI (entrega de valor, gerenciamento de risco, alinhamento estratégico, gestão de recursos e medição de desempenho) aplicados aos programas e políticas de governo.

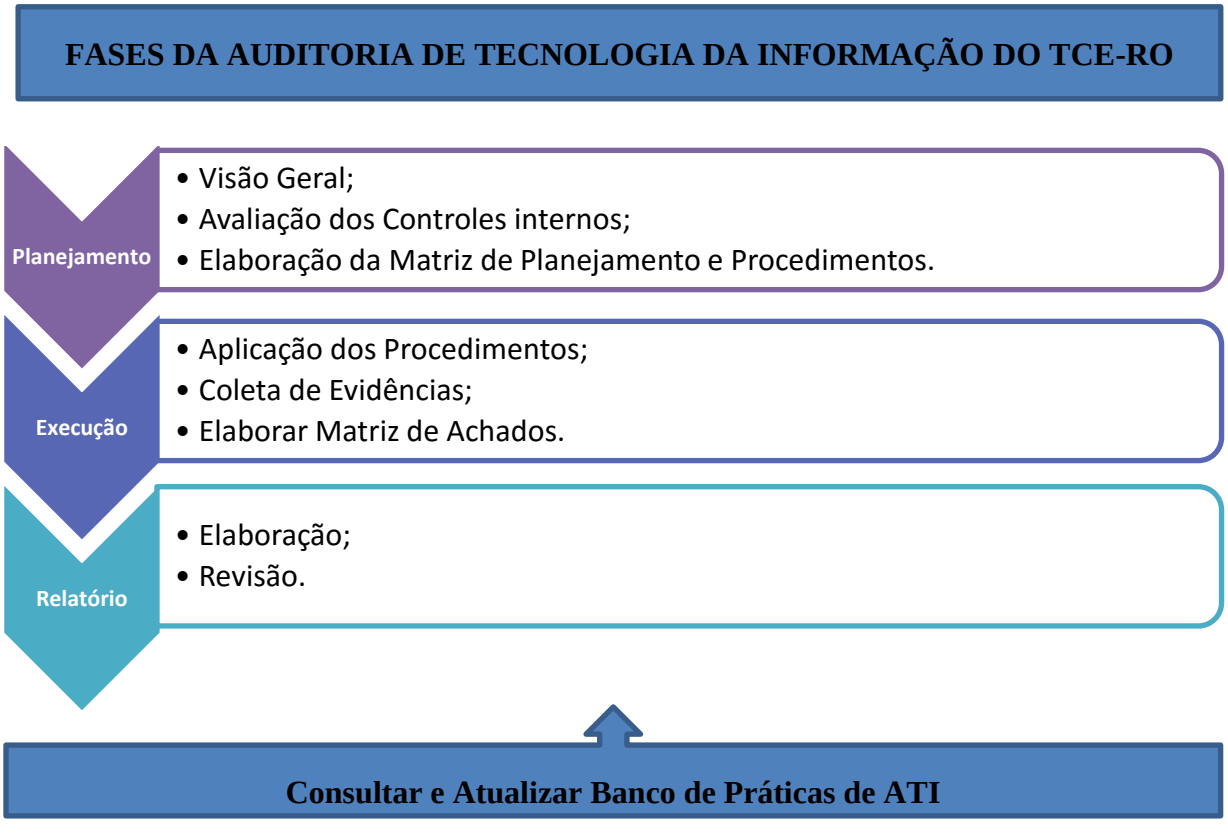
Principais enquadramentos utilizados:

- Constituição da República Federativa do Brasil de 1988, art. 37, caput (princípio da eficiência).
- Norma Técnica Cobit 4.1 (Control Objectives for Information and Related Technology –guia de boas práticas, dirigido para a gestão de tecnologia de informação).
- Decreto estadual que trate sobre temas correlatos.

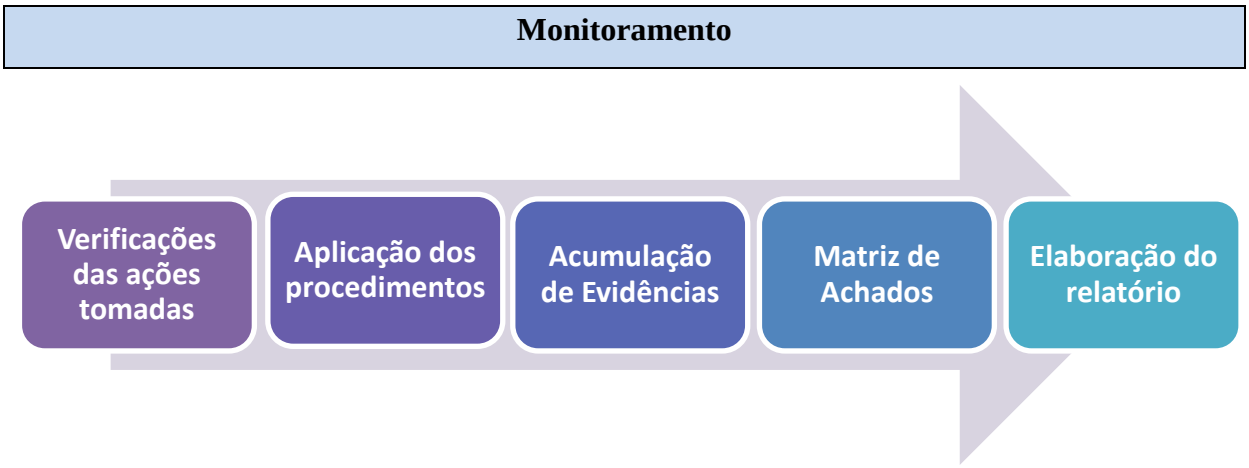
3. MÉTODO DE TRABALHO

3.1 FASES DA AUDITORIA

As fases de Auditoria de TI são: Planejamento, Execução e Relatório. Cada uma delas possui seus instrumentos e ferramentas de trabalho. O gráfico abaixo resume as fases e etapas da Auditoria de TI. A etapa de Consultar e Atualizar o Banco de Práticas para Auditoria de TI é a única que é realizada em todas as fases da auditoria e por este motivo é colocada em seção separada (ver item 3.2).



Há de se levar em consideração, ainda, o acompanhamento das ações tomadas em resposta aos apontamentos da auditoria. Na Auditoria Tradicional, ele se dará em próximo acompanhamento de gestão. Na Auditoria Operacional, o acompanhamento se dará na fase de Monitoramento, cujo fluxo de atividades é apresentado abaixo:



3.1.1 PLANEJAMENTO

Nesta fase, devem ser definidos: objetivo da auditoria, universo a ser auditado (escopo), técnicas e procedimentos a serem utilizados, critérios de auditoria, etapas, cronograma, recursos humanos e materiais. A fase de Planejamento por sua vez está dividida nas seguintes etapas: Visão Geral, Avaliação do Controle Interno e Elaboração da Matriz de Planejamento e Procedimentos.

a) Visão Geral

Etapa que consiste em conhecer o ente que se vai auditar. Devem ser identificados os objetivos institucionais do ente; a estrutura organizacional; a legislação aplicável; as práticas administrativas; e a descrição do objeto da fiscalização (quem, qual setor).

Fontes de informações possíveis: levantamento de auditorias anteriores, relatórios de auditoria realizadas, relatórios de auditoria interna, discussão com a gerência e com outros auditores que já realizaram trabalhos no ente, orçamento do ente, documentos de

estratégia de TI ou plano diretor de TI, legislação e normas aplicáveis, entrevistas, internet e bases de conhecimento de ATI.

b) Avaliação dos Controles Internos

É um instrumento que precisa ser desenvolvido junto aos órgãos jurisdicionados com o intuito de minimizar problemas encontrados em cada uma das abordagens. Tal trabalho poderia ser facilitado a partir de um trabalho desenvolvido pelo Tribunal de Contas com o foco em Governança de TI.

c) Elaboração da Matriz de Planejamento e Procedimentos

É o instrumento para organizar as informações relevantes do planejamento de uma auditoria. Permite o entendimento da equipe em relação ao objetivo do trabalho, aos passos a serem seguidos e à estratégia metodológica a ser adotada. Orienta os integrantes da equipe nas fases de execução e de elaboração do relatório. Para sua elaboração pode ser consultado o Banco de Questões de Auditoria. (ver item 3.2.1).

Matriz de Planejamento

Objetivo: Enunciar de forma clara e resumida o objetivo da auditoria

Nº	Questões de Auditoria	Informações Requeridas	Fontes de Informações	Possíveis Achados
Q1	[Apresentar em formas de perguntas os aspectos a serem investigados para atingir o objetivo da auditoria]	[Identificar as informações e fontes necessárias para responder a questão de auditoria]	[Identificar as fontes de informações utilizadas para se alcançar a informação – ex: base de dados, requisições de documentos, visitas técnicas, entrevistas, ...]	[Esclarecer precisamente que conclusões ou resultados podem ser alcançados, usar a notação A1, A2, An (para possibilitar correspondência com a Matriz de Achados)]
Q...				
QN				

Outra forma de se desenvolver a mesma Matriz de Planejamento, apenas com uma forma de visualização diferente seria a seguinte:

Matriz de Planejamento

Objetivo: [Enunciar de forma clara e resumida o objetivo da auditoria]

Q1 – [Apresentar em forma de perguntas os aspectos a serem investigados para atingir o objetivo da auditoria]

Informações Requeridas	**Fontes de Informações**	**Possíveis Achados**
[Identificar as informações e fontes necessárias para responder a questão de auditoria]	[Identificar as fontes de informações utilizadas para se alcançar a informação – ex: base de dados, requisições de documentos, visitas técnicas, entrevistas, ...]	[Esclarecer precisamente que conclusões ou resultados podem ser alcançados, usar a notação A1, A2, An (para possibilitar correspondência com a Matriz de Achados)]

Forma de Preenchimento:

- Nº: Informar o número da questão no formato "Q" mais a sequência da questão.Por exemplo: questão número 1 – Q1, questão número 2 (Q2) e assim por diante.
- Questões de Auditoria: elaborar em forma de perguntas, os diferentes aspectos que compõem o escopo da auditoria e que devem ser investigados com vistas à satisfação do objetivo.
- Informações Requeridas e Fontes: identificar as informações necessárias para responder a questão de auditoria, bem como as fontes de cada item de informação;
- Possíveis Achados: identificar que conclusões ou achados podem ser encontrados.

Exemplos:

Ex. 1:

Matriz de Planejamento
Objetivo: Assegurar que o processo de desenvolvimento e manutenção de sistemas é sistematizado.

Nº	**Questões de Auditoria**	**Informações Requeridas e Fontes**	**Possíveis Achados**
Q1	Há padrões para o desenvolvimento de sistemas?	O documento que descreve o padrão.	Inexiste processo sistematizado para desenvolvimento de sistemas.
Q2	Estão previstos os artefatos a serem gerados para documentação dos sistemas?	Verificar no documento que descreve o padrão. Selecionar um sistema e verificar se foram gerados os artefatos	Inexiste ou é precária a documentação de sistemas.

Q3	Há regras para implementação de mudanças em sistemas?	Verificar no documento que descreve o padrão.	As mudanças promovidas em sistemas não são testadas ou não são homologadas em ambientes específicos antes de entrarem em produção.

Ex. 2

Matriz de Planejamento

Q1 – Existem contratos que foram firmados não respeitando os ditames legais?

Informações Requeridas	Fontes de Informações	Possíveis Achados
Relação de todos os contratos firmados pela entidade jurisdicionada auditada	Relação em meio digital ou em papel	Há contratos firmados que não respeitam a lei de licitações ou estão fora dos ditames legais

Q2 – Nos contratos de prestação de serviços, a avaliação dos preços está condizente com os preços praticados no mercado?

Informações Requeridas	Fontes de Informações	Possíveis Achados
Análise das propostas técnicas dos contratos e pesquisa e verificação de sua equidade financeira.	Análise física ou digital dos processos de contratação e consulta a internet ou contratos de outras entidades.	Os preços estão acima dos valores praticados no mercado.

Matriz de Procedimentos

Nº Questões de Auditoria	Procedimentos	Objetos	Achados
Q1	P11	[Descrição dos itens de verificação ou check-list para a questão de auditoria]	A1
	P12		
	P1N		

Forma de Preenchimento:

- ⓘ Q1: Informar o número da questão no formato "Q" mais a sequência da questão. Por exemplo: questão número 1 – Q1; questão número 2 (Q2) e assim por diante.
- ⓘ P1: Informar o número do procedimento no formato "P" mais a sequência do procedimento. Por exemplo: procedimento número 1 – P11; questão número 1 (Q1) e achado A1 do procedimento 1 e assim por diante.
- ⓘ Procedimentos de Auditoria: descrição dos itens de verificação ou checklist. Usar notação P11, P12,..., P1n, onde o primeiro algarismo corresponde à questão de auditoria e os próximos ao número do procedimento de forma sequencial e crescente, reiniciando a cada questão.
- ⓘ Achados: Informar o número do achado no formato "A" mais a sequência do achado de auditoria. Por exemplo: achado número 1 – A1; achado número 2 (A2) e assim por diante.

Exemplos:

Matriz de Procedimentos

Questões de Auditoria	Procedimentos	Objetos	Achados
Q1	P11	Requisitar, através de uma Requisição de Documentos e/ou Informações todos os contratos de TI firmados pela entidade jurisdicionada dentro do período de exercício auditado	
	P12	Analisar a listagem e filtrar os contratos que tenham valores expressivos ou significativos e selecionar também contratos que possuam algum indício de problema ou uma descrição mal elaborada	
	P13	Analisar os contratos e verificar se a contratação foi desenvolvida respeitando as normas legais – LF 8.666/93, analisando o prazo, objeto, documentação comprobatória, termos aditivos, responsáveis e fiscais do contrato, cronograma de pagamentos, justificativas para a contratação, verificação do que foi entregue – termo de aceite, verificação de como foi desenvolvido o processo de gestão contratual e verificação se ambas as partes estão cumprindo ou cumpriram o acordado.	A1

3.1.2 Execução

a. Aplicação dos Procedimentos (descritos na matriz de planejamento e procedimentos): os procedimentos elencados na coluna "Objetos" da Matriz de Planejamento

são aplicados no ambiente da auditada, para a aquisição e a coleta das informações que servirão como evidências de auditoria.

b. Acumulação de Evidências: as informações levantadas a partir da aplicação dos procedimentos são organizadas e acumuladas, a fim de identificar e documentar os achados de auditoria identificados na coluna "Achados" da Matriz de Planejamento.

c. Desenvolvimento Matriz de Achados: Como resultado da aplicação dos procedimentos relacionados na coluna "Objetos" da Matriz de Planejamento, podem ser identificados os achados relacionados na coluna "Achados" da Matriz. Esses achados, cuja documentação comprobatória é aquela identificada durante o processo de "Acumulação de Evidências", deverão ser relacionados e descritos na Matriz de Achados.

Matriz de Achados

Objetivo: [Estruturar o achado ou recomendação]

Nº	Situação Encontrada	Critério	Evidências	Causas	Efeito	Encaminhamento
[Correspondência com o achado de Auditoria (An) da Matriz de Planejamento e Procedimentos.]	[Situação existente, identificada e documentada durante fase de execução da auditoria.]	[Legislação, norma, jurisprudência, entendimento doutrinário ou padrão adotado.]	[Informações obtidas durante a auditoria no intuito de documentar os achados e de respaldar as opiniões e conclusões da equipe.]	[O que motivou a ocorrência do achado.]	[Consequências reais ou potenciais do achado.]	[Proposta da equipe de auditoria. Deve conter achado ou recomendação, dependendo da situação e do tipo de auditoria.]
A1						
[AN]						

Forma de Preenchimento:

- Nº: Informar o número do Achado no formato "A" mais a sequência do achado. Por exemplo: achado número 1 – A1; achado número 2 (A2) e assim por diante.
- Situação Encontrada: descrever a situação encontrada, identificada e documentada durante a fase de execução da auditoria.
- Critério: elencar os critérios que sustentam o apontamento. Podem ser normas técnicas, legislação, entendimento doutrinário.
- Evidência: documentos obtidos durante a auditoria que comprovam e sustentam as conclusões da equipe.
- Causas: descrever as causas que resultaram nos problemas encontrados; o que foi feito, ou deixou de ser feito, e que resultou no efeito encontrado.
- Efeito: as consequências que ocorrem em virtude do Achado.
- Encaminhamento: propostas da equipe para encaminhamento para o achado encontrado. Pode ser uma recomendação, determinação, etc.

3.1.3 Relatório/Folhas de Instrução e Revisões

a. Elaboração do Relatório: O Relatório de Auditoria dos processos de Auditoria de TI não difere daqueles elaborados em processos de auditoria ordinária tradicional, e deve estar de acordo com as orientações descritas na seção 9.5 do manual MT-DCF-195. Para a elaboração do Relatório, deverão ser utilizados os elementos levantados durante a elaboração das matrizes descritas na seção anterior, em especial a Matriz de Achados.

O Relatório será desenvolvido e elaborado seguindo a seguinte estrutura:

R.1 - a introdução ao apontamento será elaborada a partir da coluna "Situação Encontrada" da Matriz de Achados;

R.2 - as causas do apontamento e as consequências da sua ocorrência serão elaboradas a partir das colunas "Causas" e "Efeitos" da Matriz de Achados;

R.3 - o processo de descoberta e identificação da irregularidade serão descritas com base no conteúdo da coluna "Evidências" das Matriz de Achados;

R.4 - o conteúdo da coluna "Critérios" será usado para descrever e detalhar quais os dispositivos legais, normas e padrões que estão sendo infringidos na ocorrência da irregularidade;

R.5 - por fim, os apontamentos da Equipe de Auditoria serão elaboradas a partir do conteúdo da coluna "Encaminhamento" da Matriz de Achados.

Deve-se, durante a execução desse processo, buscar a elaboração do relatório de forma lógica, coerente, estruturada e fácil de ser compreendida.

b. Folhas de Instrução: As Folhas de Instrução conterão a reprodução fiel das matrizes elencadas nesse documento, quais sejam: Matriz de Planejamento, Matriz de Procedimentos e Matriz de Achados. Podem ser agregadas novas informações referentes a processos e contratos, a título explicativo e auxiliar no trabalho de auditoria.

c. Revisão: A revisão deve levar em consideração a estrutura do relatório e das folhas de instrução, avaliando se a correspondência e o embasamento legal estão bem construídos.

3.2 Banco de Práticas de ATI

O Banco de Práticas de Auditoria de TI visa centralizar, captar e disseminar o conhecimento gerado durante e após uma auditoria. Deve ser utilizado em todas as fases da auditoria.

Consiste em informações que auxiliam na montagem das Matrizes de Planejamento e de Achados e que mantém informações relacionadas a pessoas (gestores, prepostos, sócios de empresas, agentes públicos), entes, empresas, entendimentos e decisões, licitações e temas específicos, relacionando informações implícitas que podem indicar e subsidiar um possível Achado.

3.2.1 Banco de Questões

Contém lista pré-definida com questões básicas que auxiliam a montagem da Matriz de Planejamento e Procedimentos.

3.2.2 Banco de Inconformidades

Contém lista pré-definida com as principais inconformidades contendo todos os atributos que completam um achado: Critérios, Causas, Efeitos e Encaminhamentos.

3.2.3 Banco de Relatos de Auditoria

Contém de forma organizada informações de Órgãos e Entidades, Relacionamentos e Atributos identificados em um ambiente de Tecnologia da Informação. Exemplo: Empresas e Sócios, Empresas e Órgãos que já se relacionaram, Processos Licitatórios que a empresa já participou, Empresas ou Órgãos nos quais o agente público já trabalhou, etc.

3.3 Canais de Comunicação

A Auditoria de TI estabeleceu dois canais de comunicação interna, quais sejam:

1. Intranet – tem como objetivo divulgar informações que tem como público alvo, principalmente, a Casa como um todo.

Acesso: http://intranet

2. Fórum – tem como objetivo centralizar a discussão de assuntos polêmicos ou triviais para consenso (ou não). Após o entendimento a informação deve ser transferida para a Base de Conhecimento adequada.

REFERÊNCIAS

BRASIL, TCU.

RIO GRANDE DO SUL, Tribunal de Contas do.

CEARÁ, Tribunal de Contas do.

PERNAMBUCO, Tribunal de Contas do.

GOLDSCHIMIDT, Frederico: Auditoria em TI: Alternativas de Implementação no Processo de Auditoria do TCE-RO.

CÂNDIDO, Elaine AUDITORIA EM SISTEMAS DE INFORMAÇÃO E A APLICAÇÃO DA NORMA ISO 27002:2005.

PACHECO, André Luiz Pacheco. Curso de Auditoria de TI. Escola Nacional de Governo. 2011.