# MANUAL DE AUDITORIA EM TI 2018

TRIBUNAL DE CONTAS DO ESTADO DO AMAZONAS

**TRIBUNAL DE CONTAS DO ESTADO DO AMAZONAS**
**Secretaria Geral de Controle Externo**
**Diretoria de Controle Externo em Tecnologia da Informação**

# MANUAL DE AUDITORIA DE TECNOLOGIA DA INFORMAÇÃO TRIBUNAL DE CONTAS DO ESTADO DO AMAZONAS

## CONSELHEIROS

Cons. Yara Amazônia Lins Rodrigues dos Santos
Presidente

Cons. Mario Manoel Coelho de Mello
Vice-Presidente

Cons. Antonio Julio Bernardo Cabral
Corregedor

Cons. Érico Xavier Desterro e Silva
Ouvidor

Cons. Ari Jorge Moutinho da Costa Júnior
Cons. Josué Cláudio de Souza Filho
Cons. Júlio Assis Corrêa Pinheiro
Conselheiros

Mário José de Moraes Costa Filho
Alípio Reis Firmo Filho
Luiz Henrique Pereira Mendes
Auditores

## SECRETÁRIO-GERAL DE CONTROLE EXTERNO

Stanley Scherrer de Castro Leite

## EQUIPE DIATI

Álvaro Ramos de Medeiros Raposo
Weslei José de Paula
Mário Augusto Takumi Sato

**TRIBUNAL DE CONTAS DO ESTADO DO AMAZONAS**
**Secretaria Geral de Controle Externo**
**Diretoria de Controle Externo em Tecnologia da Informação**

# SUMÁRIO

# ÍNDICE DE ILUSTRAÇÕES

# ÍNDICE DE TABELAS

# LISTA DE ABREVIAÇÕES

| | | |
|---|---|---|
| ACL | - | Linguagem de Comandos de Auditoria (em inglês) |
| BCP | - | Processo de Continuidade de Negócio (em inglês) |
| CMMI | - | Modelo Integrado de Maturidade em Capacitação (em inglês) |
| COBIT | - | Objetivos de Controle para Informação e Tecnologias Relacionadas (em inglês) |
| DIATI | - | Diretoria de Controle Externo em Auditoria de Tecnologia da Informação |
| DOD | - | Documento de Oficialização da Demanda |
| DRP | - | Processo de Recuperação de Desastres (em inglês) |
| IDEA | - | Extração e Análise de Dados Interativa (em inglês) |
| IEC | - | Comissão Eletrotécnica Internacional (em inglês) |
| INTOSAI | - | Organização Internacional das Entidades Fiscalizadoras Superiores |
| ISACA | - | Associação de Auditoria e Controle de Sistemas da Informação (em inglês) |
| ISO | - | Organização Internacional de Padronização |
| ISSAI | - | Normas Internacionais das Entidades Fiscalizadoras Superiores (em inglês) |
| ITIL | - | Biblioteca de Infraestrutura em Tecnologia da Informaçã9 (em inglês) |
| KPI | - | Indicadores-chave de processo |
| NBR | - | Normas Brasileiras |
| PB | - | Projeto Básico |
| SLA | - | Acordo de Nível de Serviço (em inglês) |
| TCE/AM | - | Tribunal de Contas do Estado do Amazonas |
| TI | - | Tecnologia da Informação |
| TR | - | Termo de Referência |

## INTRODUÇÃO

O advento da Tecnologia da Informação mudou a maneira como trabalhamos em vários aspectos, e a atividade de auditoria também segue essa regra. No entanto, a onipresença da informática, enquanto uma das mais efetivas ferramentas organizacionais, também trouxe consigo várias vulnerabilidades inerentes a um ambiente organizacional automatizado. Cada nova vulnerabilidade precisa ser identificada, mitigada e controlada, para isso a avaliação da eficiência e efetividade de cada controle empregado requer novos métodos de auditoria.

A Tecnologia da Informação automatizou a coleta, armazenamento e provimento de pronto acesso a incontáveis quantidades de informação que são, então, usadas nas tomadas de decisão e operacionalização dos processos básicos de uma organização.

Com a criação e popularização das redes de computadores, Sistemas Computacionais passaram a ser chamados de Sistemas da Informação. Como reflexo dessa evolução, o termo Auditoria de Processamento de Dados Eletrônicos foi amplamente reformulada e, consequentemente, rebatizada como Auditoria de Tecnologia de Informação (IT PEDIA, 2017).

O aumento do investimento e da dependência em sistemas eletrônicos por parte da Administração Pública como um todo, tornou imperativo ao Analista de Controle Externo em TI a adoção de metodologia e abordagem apropriadas para que, com isso, possa identificar riscos à integridade de dados, abuso e privacidade, bem como prover a garantia de que controles sejam estabelecidos. Um Sistema da Informação quando implantado em um ambiente com controles inadequados oferece sérios riscos à Administração, dessa maneira um Auditor de TI deve ser capaz de identifica-los de modo a orientar para as melhores práticas.

Esse manual pretende prover, aos Auditores de Tecnologia da Informação do Tribunal de Contas do Estado do Amazonas e demais partes interessadas, orientações descritivas em diferentes domínios dessa disciplina,

assim como um passo-a-passo em como planejar essas auditorias de maneira efetiva.

O Capítulo 1 deste Manual resume a definição de Auditoria de TI, o escopo e objetivos das Auditorias em TI. Ele também oferece uma explicação sobre Controles Gerais de TI e Controles de Aplicação bem como estes se inter-relacionam. O Capítulo 1 também descreve o processo de auditoria de TI e a metodologia de avaliação baseada em riscos para selecionar as Auditorias de TI.

Os Capítulos de 2 a 8 mostram uma descrição detalhada de diferentes domínios de TI que irão auxiliar os Analistas na identificação de potenciais áreas de auditoria. Riscos Organizacionais relacionados ao domínio da TI foram listados no fim de cada capítulo, o que auxiliará na identificação de potenciais áreas para realização de auditorias. As orientações dadas em cada domínio ajudarão no planejamento de suas fiscalizações, seja em um domínio específico ou em uma combinação de domínios, dependendo do escopo e objetivo planejados.

Cada capítulo é apoiado por sugestões de matrizes de planejamento anexas a esse manual. As matrizes listam questões-chave, critérios, informações exigidas e métodos de análise. Usuários devem notar que as questões de auditoria listadas nas matrizes de acordo com os requerimentos específicos de suas auditorias. O modelo da matriz de planejamento é feito de forma genérica para que possa ser usado como papel de trabalho desse Tribunal.

Este Manual inclui ainda um apanhado geral sobre áreas de auditorias de TI em ascensão. O Capítulo 9 destaca algumas áreas que podem ser de interesse de auditores de TI, como sítios web, portais, governo eletrônico, auditoria baseada em computação forense e computação móvel.

Por fim, cabe ainda ressaltar que o presente Manual segue princípios gerais de auditoria baseados em Padrões Internacionais para Instituições Superiores em Auditoria (ISSAI), bem como as práticas presentes em Frameworks Internacionais de TI reconhecidos, incluindo o Framework Cobit da ISACA, Padrões ISO (International Standards Organization), entre outros. Assim, espera-se que os Analistas de Controle Externo do Tribunal de

Contas do Estado do Amazonas, bem como demais servidores interessados encontrem nesse Manual uma ferramenta útil na evolução de seus conhecimentos bem como auxilie no planejamento de suas auditorias.

# 1. AUDITORIA DE TECNOLOGIA DA INFORMAÇÃO

Por conta das inovações trazidas pelo desenvolvimento tecnológico, as organizações investem cada vez mais em automatização de atividades e em gestão da informação. Com isso, cria-se um cenário em que o uso desses dados torna auditorias cada vez mais estruturadas.

## 1.1 O QUE É AUDITORIA DE TI

Auditoria de TI é o processo de garantir que o desenvolvimento, a implantação e a manutenção de Sistemas de TI atingem os objetivos da organização, zelam pelo uso de ativos e mantém a integridade dos dados. Em outras palavras, a Auditoria de TI é a fiscalização de Sistemas e Controles de TI para assegurar que supram as necessidades da organização sem comprometer a segurança, privacidade, custo e outros elementos.

O Guia para Auditoria de TI da Organização Internacional das Entidades de Fiscalização Superiores (INTOSAI, 2013) define auditoria de TI como:

> *"Um exame e revisão de sistemas de TI e controles relacionados para obter garantia ou identificar violações dos princípios de legalidade, eficiência, economia e eficácia do sistema de TI e controles relacionados.".*

### 1.1.1 Competência para Auditoria de TI

A competência para o TCE/AM conduzir uma Auditoria de TI é extensão da competência geral atribuída a esta Corte para conduzir auditorias financeiras, de conformidade, operacional ou uma combinação destas, conforme recomenda a ISSAI 5300 que versa sobre Diretrizes para Auditoria de TI (INTOSAI, 2016), e como tal é prevista em seu Regimento Interno (TCE/AM, 2002), mais precisamente no art. 5º que enuncia:

> "*Art. 5º. Compete ao Tribunal:*
>
> *VII - realizar, por iniciativa própria, da Assembléia Legislativa ou de Câmara Municipal, de comissão técnica ou de inquérito, inspeções e auditorias de natureza contábil, financeira, orçamentária, operacional e patrimonial nos órgãos dos Poderes Legislativo, Executivo, Judiciário, do*

> *Ministério Público e demais entidades referidas no inciso II deste artigo, o Tribunal de Contas, inclusive*
> *X - prestar as informações solicitadas pela Assembléia Legislativa, por Câmara Municipal ou por comissão técnica sobre a fiscalização contábil, financeira, orçamentária, operacional e patrimonial, bem como sobre resultados de auditorias e inspeções realizadas;*
> *XI - aplicar aos responsáveis, em caso de ilegalidade de despesa ou irregularidade de contas, as sanções previstas em lei;*".

### 1.1.2 Objetivos de Auditorias de TI

A Organização Internacional das Entidades Fiscalizadoras Superiores (INTOSAI, em inglês), que reúne as principais Entidades Superiores em Auditoria, grupo do qual o Tribunal de Contas da União faz parte, emitiu a seguinte afirmação constante na Declaração de Lima, carta que reúne os princípios e diretrizes de auditoria (INTOSAI, 1977):

> "*Os consideráveis gastos investidos no processamento eletrônico de dados demandam por auditorias apropriadas. Tais auditorias devem ser baseadas em sistemas e abranger aspectos, tais como planejamento, uso econômico dos equipamentos de processamento de dados; alocação de pessoal com habilidades apropriadas, preferencialmente dentro da administração da organização auditada; prevenção ao mau uso; e utilidade da informação produzida;*".

Assim, o objetivo das Auditorias de TI é de assegurar que as melhores práticas estejam empregas visando o atendimento das necessidades organizacionais de maneira eficiente, eficaz e econômica, podendo abranger auditorias de Sistemas da Informação, Desenvolvimento desses Sistemas, Segurança de TI, Aquisição de Bens e Serviços, Continuidade de Negócio, entre outras.

Segundo (Auditor-General's Office Singapore, 2009) a importância das Auditorias de TI pode ser resumida em:

- Aumento da quantidade, extensão e complexidade dos mecanismos de controle organizacionais.
- Aumento do impacto da TI na forma como os entes fiscalizadores exercem suas competências.

- Jurisdicionados cada vez mais automatizados, por consequência, sujeitos a maiores riscos relacionados à complexidade da TI.
- Novos conceitos e metodologias de trabalho.
- Controles Internos cada vez mais implementados em sistemas da informação.

### 1.1.3 O Escopo das Auditorias de TI

O Analista Técnico de Controle Externo que atuar em fiscalizações da área de tecnologia deve avaliar as políticas e procedimentos que guiam o ambiente geral de TI do órgão auditado, assegurando que os controles e mecanismos de coerção estejam estabelecidos.

A definição do escopo da auditoria de TI se dá basicamente na delimitação da abrangência de sua avaliação, que segundo (BERGAMI, 2013) pode abarcar:

- Processos de negócio apoiados em TI;
- Governança e Gestão de TI;
- Aquisições de TI;
- Contratos de prestação de serviços de TI;
- Sistemas da Informação;
- Bancos de dados;
- Segurança da Informação;
- Infraestrutura física.

Para analisar esses vários segmentos de tecnologia a Auditoria de TI deve avaliar:

- A confiabilidade de informações processadas por sistemas;
- A segurança física do ambiente de processamento de TI de uma organização;
- A conformidade do funcionamento de um sistema em relação a normas, padrões e resultados esperados.
- A adequação da infraestrutura da área de TI para o processamento dos sistemas e informações;

- A qualidade dos produtos, dos sistemas e dos serviços oferecidos pela área de TI ao negócio;
- A legalidade e eficiência da contratação de bens e serviços de TI por parte da organização.

### 1.1.4 Controles de TI

Um controle é a combinação de métodos, políticas e procedimentos que asseguram a proteção dos ativos da organização, a exatidão e a confiabilidade de seus registros bem como a aderência operacional aos padrões de gerenciamento.

Segundo (INTOSAI, 2013) em um contexto de TI, controles são divididos em duas categorias, de acordo com seu alcance e influência e sua relação a alguma aplicação em particular: controles gerais de TI e controles de aplicação.


Figura 1 - Controles Gerais de TI

Os Controles Gerais são base da estrutura de Controles de Tecnologia da Informação. Eles se preocupam com o ambiente geral em que os Sistemas da Informação são desenvolvidos, operados, gerenciados e mantidos. Controles Gerais de TI estabelecem um framework para as atividades de TI e oferecem garantias de que os objetivos gerais de controle sejam satisfeitos.

Eles são desenvolvidos com base em políticas, orientações e procedimentos, assim como o estabelecimento de uma estrutura e gerenciamento, que engloba o gerenciamento dos Sistemas da Informação da entidade (NUNES, 2012).

Exemplos de controles gerais incluem o desenvolvimento e a implementação de uma Estratégia de Sistemas da Informação e Política de Segurança de Sistemas da Informação, a criação de um Comitê Geral de TI, organização da equipe de sistemas da informação para separar atividades conflitantes, e planejamento para prevenção e recuperação de desastres.

Controles de Aplicação são controles específicos para cada Sistema da Informação e estão relacionados às transações dos dados existentes. Controles de Aplicação incluem validação de dados de entrada, criptografia dos dados a serem transmitidos, controles de processamento e etc. Por exemplo, em uma aplicação que demande pagamento online, um controle de entrada poderia ser que a data de validade do cartão de crédito seja após a data da transação, e detalhes inseridos deveriam ser criptografados.

### 1.1.5 Controles de Gerais de TI, Controles de Aplicação e seus Relacionamentos

O objetivo dos Controles Gerais de TI é assegurar o desenvolvimento e implementação de aplicações eficientes e efetivas, assim como que a utilização destas resulte em dados relevantes que sejam armazenados em banco de dados, em arquivos ou ainda sirva como parâmetro de entrada para interações com outras aplicações (INTOSAI, 2013).

O projeto e a implementação de Controles Gerais de TI podem ter um impacto significativo na efetividade dos controles de aplicação, pois fornecem os recursos necessários às aplicações para que operem e evitem que mudanças não autorizadas sejam feitas.

Os Controles Gerais de TI mais comuns são:

- Controle de Acesso Lógico sobre infraestrutura, aplicações e dados
- Controles de Ciclo de Vida de Desenvolvimento de Sistemas
- Controles de Gerenciamento de Mudança de Programas
- Controles de acesso físico sobre Data Center

- Back-up de Dados e Sistemas e Controles de Recuperação
- Controles de Operação de Computadores

Já os Controles de Aplicação operam em transações individuais e asseguram que dados de entrada, processamento e saída sejam corretos. A efetividade de projeto e implantação de Controles Gerais de TI tem grande influência sobre a extensão dos controles de aplicação estabelecidos pelo gerenciamento para o tratamento de riscos.

#### 1.1.5.1 Controles de TI importantes para o Analista

Enquanto a Auditoria Governamental avalia controles de financeiros, regulatórios e de conformidade, a atuação do Auditor de TI se baseia no teste dos controles relacionados às tecnologias utilizadas nos processos organizacionais. Posto que cada vez mais organizações confiam à TI a automação de suas atividades, a linha divisória do papel de um Auditor de TI e Auditoria Governamental vem reduzindo gradativamente.

Hoje, os auditores são requisitados a entender o ambiente de controle da entidade auditada para assim garantir a operacionalidade de seus controles internos. Como afirmam os Princípios Fundamentais da Auditoria no Setor Público da ISSAI: *"Auditores devem obter um entendimento da natureza da entidade/programa a ser auditado"* (INTOSAI, 2013). Isso inclui um entendimento dos Controles Internos, assim como objetivos, operações, ambiente regulatório, sistemas e processos de negócio envolvidos.

Cada Área de Controle se baseia em um conjunto de objetivos e riscos. O papel do auditor é compreender esses potenciais riscos de negócio inerentes a TI e avaliar se os controles implementados pela organização são adequados para alcançar seus objetivos.

No caso dos Controles Gerais de TI é importante para o auditor a compreensão da ampla gama de categorias, a extensão dos controles em operação e encontrar o quão efetivos são esses controles de forma a entregar as garantias que se propõem, bem como a avaliação do gerenciamento da equipe operacional. A ISSAI 1315 aponta que mesmo pequenas entidades onde sistemas da informação e processos de negócio relevantes para gestão

financeira são menos sofisticados, o papel dos Controles Gerais de TI é significativo (INTOSAI, 2014). Se esses controles são fracos há uma sensível diminuição da confiabilidade operacional associada as aplicações de TI.

## 1.2 O PROCESSO DE AUDITORIA DE TI

O Planejamento da Auditoria é parte fundamental de qualquer fiscalização, na Auditoria de TI não é diferente. Na maioria das organizações de controle, o planejamento de auditoria se desenvolve em três níveis – Planejamento Estratégico, Planejamento Tático/Anual e Planejamento Individual/Nível de Entidade (SEBRAE, 2017).

### 1.2.1 Planejamento Estratégico

O Planejamento Estratégico de um Órgão de Controle é uma estimativa de longo prazo, normalmente de três a seis anos, que compreende estabelece a missão e valores organizacionais bem como sua visão de futuro, resultados esperados para a sociedade bem como diretrizes para seus processos internos, gestão de pessoas e da inovação.

Essa visão de longo prazo auxilia a resposta de questionamentos tais quais:

- Aonde se pretende chegar com uma fiscalização de TI?
- De que forma é necessário se preparar para fiscalizar TI daqui a ‘X’ anos?
- Quais são as competências que necessitam ser desenvolvidas em longo prazo?
- Como acompanhar as transformações pelas quais passam a organização e o cenário em que ela atua?

O alinhamento da diretoria de Auditoria de TI com o Planejamento Estratégico do órgão de controle auxilia no diagnóstico de uma série de fatores, entre os quais:

- Pontos fracos atuais da auditoria de TI na organização;
- Demandas por treinamento e capacitação;

- Incorporação de novos métodos e técnicas para acompanhar mudanças nas demandas por auditoria;
- Adaptação às mudanças tecnológicas;
- Acompanhamento das mudanças organizacionais;
- Desenvolvimento da infraestrutura necessária (instalações físicas, software, hardware, etc).

### 1.2.2 Planejamento Tático Anual

O nível tático de um planejamento de auditoria é desenvolvido com base em Ciclos Anuais para a seleção das áreas de fiscalização. Com a rápida proliferação de modernos Sistemas da Informação nas entidades governamentais e a limitação de recursos disponíveis, uma abordagem baseada em riscos para priorizar e selecionar tópicos adequados deve ser adotada.

#### 1.2.2.1 Abordagem Baseada em Riscos

Um Tribunal de Contas tem sob sua jurisdição organizações que fazem uso da Tecnologia da Informação com vistas a desempenhar funções e atividades das mais diversas de forma que existe um número relevante de parques tecnológicos em diferentes localizações geográficas.

Riscos inerentes a TI impactam sistemas e infraestruturas de maneiras diferentes, por exemplo, a indisponibilidade, mesmo que momentânea, de um sistema pode ser crítica dependendo de onde ele ocorre. Risco de modificações não autorizadas podem originar fraudes e potenciais perdas. Os ambientes técnicos nos quais os sistemas executam também oferecem risco associado aos sistemas.

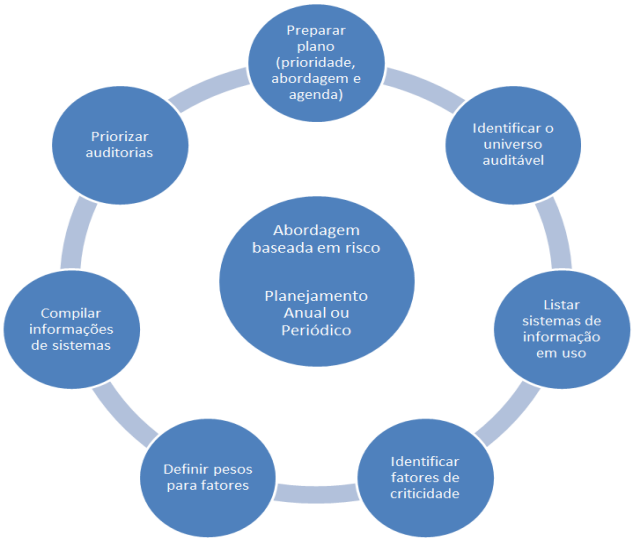


Figura 2 - Ciclo de Análise de Riscos

Uma abordagem baseada em riscos na seleção da área de TI a ser auditada é fundamental na priorização das fiscalizações. Para estabelecer uma estrutura de avaliação de riscos, um órgão de controle necessita de informações mínimas de seus jurisdicionados, normalmente reunidas mediante pesquisas (Strong Security, 2017).

Enquanto um processo de avaliação de riscos é uma maneira de selecionar a entidade auditada, o Tribunal de Contas também seleciona entidades auditáveis em uma base cíclica, usando auditorias previamente designadas ou requeridas por demais áreas de sua estrutura organizacional.

#### 1.2.2.2 Passos da Abordagem Baseada em Riscos

1. Identifique o universo de auditoria a partir de uma listagem de todas as organizações ou unidades auditáveis sob a jurisdição do órgão de controle.
2. Liste os sistemas de informação em uso nas organizações.
3. Identifique os fatores que afetam a criticidade do sistema no desenvolvimento funções e fornecimento de serviços organizacionais.
4. Atribua peso aos fatores críticos. Isso pode ser feito em consulta com a organização auditada.

5. Compile informações para todos os sistemas, em todas as organizações e com base em pontuações cumulativas, coloque os sistemas / organizações em ordem de prioridade para auditoria.
6. Prepare um plano de auditoria anual que descreva a priorização, a abordagem e o cronograma das auditorias.

### 1.2.3 Planejamento Individual

O planejamento individual envolve o desenvolvimento de um plano de auditoria detalhado para a entidade selecionada, começando pelo delineamento de objetivos de fiscalização. Os planos de auditoria vão auxiliar no preparo de um programa de auditorias de TI (INTOSAI, 2013).

Outro passo necessário para o desenvolvimento de um programa auditoria é ter uma ampla compreensão da entidade auditada e seus Objetos de Tecnologia da Informação. Planejamentos de nível individual requerem uma compreensão da organização e avaliação preliminar dos controles para facilitar o planejamento detalhado das auditorias e o preenchimento das devidas Matrizes de Planejamento.

#### 1.2.3.1 Compreendendo a Organização

A extensão do conhecimento sobre a organização e seus processos são, em sua maioria, determinados pela natureza da organização e o nível de detalhe no qual o trabalho de auditoria será realizado (DUTRA, 2017).

A avaliação prévia da organização deve ser capaz de levantar dados sobre atividades, finanças, riscos inerentes enfrentados e seus objetos de TI. Também deve incluir a extensão do quanto à organização delega de suas atividades à terceirização e em que medida os processos de negócios foram mapeados em um ambiente de TI. O auditor deve usar essa informação na identificação de potenciais problemas, formulando objetivos e o escopo do trabalho considerando ações de gerenciamento que a organização deve adotar e monitorar.

Um típico layout do uso da TI em uma organização é dado abaixo:

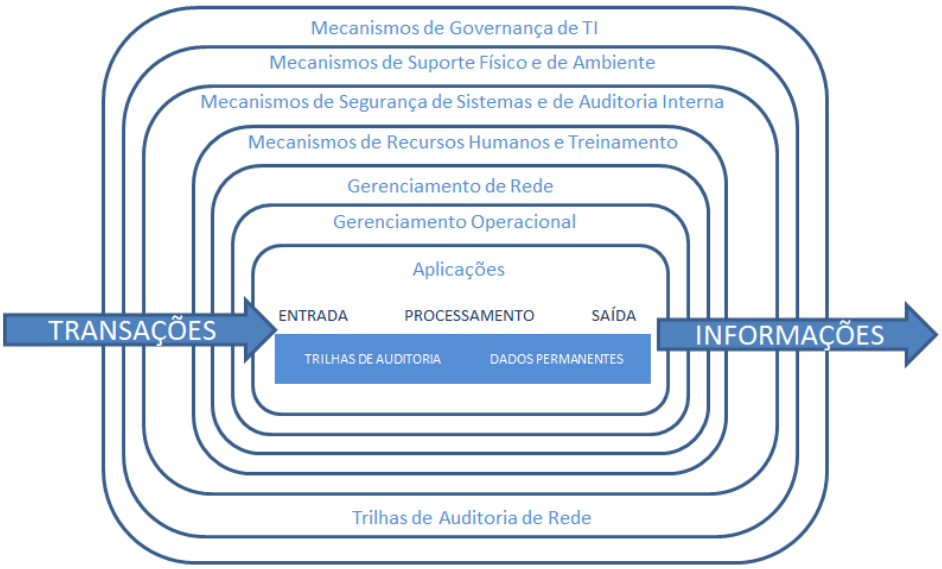


**Figura 3 - Layout de TI típico de uma organização**

Com sistemas da informação formando núcleo de uma Infraestrutura de TI, a gestão de TI abrangerá também sistemas de gerenciamento de banco de dados, controle de acesso do usuário e sistemas de gerenciamento de rede formando, assim, um ambiente interconectado.

Banco de dados e aplicações residem em servidores, que na sua essência são computadores com alta capacidade capazes de hospedar múltiplos sistemas. Os servidores poderiam ser específicos para diferentes necessidades como servidores de dados, servidores de aplicação, servidores de internet e servidores proxy.

Portanto, baseado na compreensão adquirida da Estrutura de Tecnologia da Informação da Entidade Auditada, os Auditores de TI devem definir sua abordagem de fiscalização.

#### 1.2.3.2 Materialidade

A materialidade das questões de Auditoria de TI deve ser determinada levando em conta a estrutura do órgão de controle e o contexto das declarações financeiras, natureza ou atividade da entidade auditada (INTOSAI, 2016).

O auditor de TI deve determinar se uma deficiência no processo de aquisição ou no uso da TI tem o potencial de se tornar materialmente relevante.

Por exemplo, se uma deficiência em uma aplicação tem origem em um controle geral de TI, este deve ser avaliado quanto ao impacto geral no processo envolvido para assim definir a relevância da auditoria baseada nos riscos para o órgão auditado.

#### 1.2.3.3 Alocação de Recursos

A auditoria de TI requer alocação específica de recursos, especialmente de mão de obra, que devem possuir expertise e treinamento de nível operacional em sistemas, processos e mecanismos que governam uma infraestrutura de TI. Além de equipe adequada, orçamento, infraestrutura e outros requisitos identificados devem ser oferecidos (INTOSAI, 2013).

#### 1.2.3.4 Elaboração de Matriz de Planejamento

Durante a etapa de planejamento, é útil do desenvolvimento de uma matriz de planejamento que abranja todas as questões relevantes para a auditoria de acordo com seus objetivos seu escopo.

Em sede de Auditoria de Tecnologia da Informação, essa necessidade não é diferente, portanto, devendo adotar o procedimento de maneira o mais uniforme possível com outras Diretorias de Controle Externo.

As fontes de informação típicas em TI durante uma Auditoria podem ser (INTOSAI, 2016):

a. Diagramas de fluxos de sistema, fluxo de dados, fluxos de processo etc.
b. Documentos de desenvolvimento de sistemas como Especificação de Requisitos de Usuário.
c. Dados eletrônicos.
d. Outras informações disponíveis na organização relacionadas às suas funções, controle e sistemas de monitoramento etc., como formulários, informações orçamentárias, relatórios diversos incluindo de auditorias anteriores e de controles internos e etc.
e. Políticas, Procedimentos e outras orientações.
f. Os usuários do sistema.

As entidades auditadas têm suas próprias combinações de hardware, sistema operacional, sistemas de gerenciamento de banco de dados, software de aplicação e softwares de rede o que demanda dos auditores a capacidade de reunir informações dessas fontes para consubstanciar suas análises. Entender o funcionamento dos Sistemas da Informação e de banco de dados da organização é claramente um passo essencial, por exemplo, para extração de dados.

Os analistas devem decidir na adequabilidade do uso de uma ou mais das técnicas e garantir que elas satisfaçam os objetivos de auditoria sem impactar a integridade da infraestrutura de TI, sistemas e dados da entidade auditada.

#### 1.2.3.5 Alinhamento com o órgão auditado

A entidade auditada deve estar ciente do escopo, objetivos e os critérios de avaliação da auditoria, que devem ser discutidos sempre que necessário. A equipe de auditoria deve, se preciso, enviar um expediente visando alinhar o objetivo e o escopo para a entidade auditada onde ela pode também estabelecer os termos desse alinhamento (INTOSAI, 2013). O órgão de controle deve garantir que a devida cooperação e suporte da entidade auditada sejam devidamente solicitados para a completude da auditoria, o que pode incluir o acesso a registros e informações tanto impressas quanto eletrônicas.

#### 1.2.3.6 Reunindo evidências de auditoria

Com vistas a uma coleta eficaz de evidências de auditoria do jurisdicionado, o órgão de controle deve realizar uma avaliação prévia de seus controles de TI e assim planejar os testes que serão aplicados.

##### 1.2.3.6.1 Avaliação Preliminar de Controles de TI

Para obter a compreensão da existência e confiabilidade dos controles de TI da entidade jurisdicionada o Auditor de TI atuar por meio de (INTOSAI, 2016):

a. Avaliação do Planejamento Estratégico, Planejamento de TI do Órgão Auditado.

b. Avaliação prévia da quantidade, abrangência, criticidade e materialidade da infraestrutura de TI utilizada no órgão.
c. Avaliação do estabelecimento e operacionalidade dos mecanismos de Governança de TI.
d. Avaliação dos objetivos de TI e seu alinhamento aos objetivos de negócio.
e. Avaliação do estabelecimento dos controles necessários em todas as etapas do processo para a aquisição de uma solução de TI (abrangência, aplicações de TI, hardware, software, recursos humanos, rede, soluções de serviço, etc).
f. Avaliação dos controles das atividades operacionais diárias de TI como procedimentos de segurança da informação, procedimentos de continuidade de negócio e de backup, gerenciamento de mudanças e entrega e feedback de serviços.

Os Controles de TI acima se preocupam com a infraestrutura geral de TI da organização, incluindo políticas relacionadas a TI, procedimentos e práticas de trabalho. A partir do levantamento da infraestrutura do órgão é necessário estruturar uma medição da influência de cada fator para a consecução dos objetivos do órgão. Os testes devem ser projetados de maneira específica utilizando técnicas que incluem entrevistas, pesquisas por questionários, observação, passo-a-passo, captura de dados análises e testes, entre outras.

#### 1.2.3.6.2 Testes Substantivos

Os testes substantivos envolvem avaliações detalhadas dos Controles de TI empregando várias técnicas e ferramentas para análise, extração e análise de dados.

Análises de dados envolvem (Portal de Auditoria, 2016):

- Identificar o objetivo da análise ou projeto.
- Compreender as amostras em estudo.
- Ciência dos layouts de dados e formatos.

- Estabelecer um identificador único se a correspondência ou fusão for necessária.
- Estabelecimento das questões / objetivos de auditoria.
- Listar métodos utilizados para responder as questões de auditoria.
    - Critérios de avaliação
    - Evidências
    - Análise
    - Conclusão
- Procedimentos para restruturação de arquivos como criação de sintaxe, a adição de novas variáveis, etc.
- Procedimentos de limpeza de dados (Exemplo: remoção de valores atípicos)

Algumas análises podem exigir transformações dos dados puros, subconjuntos, ou dados de entrada específicos para atender softwares estatísticos. Sistemas de TI usam vários tipos de dados diferentes e representações (numérico, texto, alfanumérico, etc). O Analista de Controle Externo deve estar ciente disso e utilizar as ferramentas apropriadas para análise. Ele pode fazer uso de Softwares Gerais de Auditoria ou Softwares Especializados de Auditoria para efetuar a análise das operações. Ferramentas como Microsoft Excel, Microsoft Access, IDEA, ACL, entre outras, são exemplos de softwares gerais de auditoria que provém facilidade para importação e análise de dados.

A partir daí qualquer uma das técnicas abaixo, pode ser adotada por auditores de TI (INTOSAI, 2013):

a. Extração de dados por obtenção de cópia da entidade auditada. Para isso pode ser necessário:
    a. Criar ambientes similares (sistemas operacionais, sistemas de gerenciamento de banco de dados, hardware, etc.),
    b. Converter dados de uma forma a outra para facilitar a leitura e a análise.
b. Realizar testes de dados em situações onde a qualidade do programa necessita ser testada.

a. A premissa é que é possível avaliar a confiabilidade geral de um programa com um conjunto de testes específicos. O uso de testes engloba Projeto de Testes e Criação de Dados de Teste antes de execução do programa.

O Analista de Controle Externo deve selecionar a avaliação de riscos apropriada e usar técnicas de amostra para obter conclusões adequadas baseadas em checagens estatisticamente suficientes em dados limitados.

## 1.3 DOCUMENTAÇÃO DE AUDITORIA

A documentação da auditoria é um registro do trabalho realizado e as evidencias de que embasam achados e conclusões. A preservação de resultados e suas evidências deve ser garantida pelos analistas na medida em que eles estejam de acordo com a conformidade dos requisitos de confiabilidade, completude, suficiência e exatidão. Também é importante para o analista garantir que o processo de auditoria seja preservado para propiciar verificações subsequentes dos procedimentos de análise. Isso envolve técnicas de documentação adequada.

A documentação engloba registros de (INTOSAI, 2016)

- O planejamento e preparação do escopo e objetivo da auditoria.
- Os programas de auditoria.
- A evidência coletada com base nas conclusões obtidas.
- Todos os papeis de trabalho incluindo arquivos gerais pertencentes ao jurisdicionado e seus sistemas.
- Pontos discutidos em entrevistas, pessoa entrevistada, posição e atribuição, hora e lugar.
- Relatórios e dados obtidos diretamente de sistema pelo analista ou providos pela equipe auditada. O Analista deve garantir que esses relatórios sejam relevantes e que constem de data, hora e condições cobertas.
- Em vários pontos da documentação, o auditor deve adicionar seus comentários e explicações, preocupações, dúvidas e

necessidades de informações adicionais. O auditor deve retornar a esses comentários posteriormente e adicionar lembretes e referências a decisões tomadas.

- Para preservação, o órgão de controle deve providenciar backup dos dados recebidos da entidade auditada e os resultados de buscas e análises. A documentação de auditoria deve ser mantida confidencial e deve ser guardada pelo período regimental decidido pela Corte de Contas ou pela lei.
- Quando o trabalho de auditoria é revisado por um par ou superior, os comentários que surgirem devem ser acrescentados à documentação.
- O relatório preliminar e conclusivo da auditoria deve fazer parte da documentação.

## 1.4 SUPERVISÃO E REVISÃO

O trabalho da equipe de auditoria deve ser devidamente supervisionado durante, e a documentação gerada deve ser revisada e armazenada na forma regimental.

## 1.5 RELATÓRIOS

O Relatório de Auditoria de TI deve seguir o layout geral do sistema de relatórios seguidos pelo Tribunal de Contas e deve ser elaborado em linguagem adaptada ao nível de detalhe exigido e ao seu público final.

O Analista de Controle Externo deve relatar seus achados em uma maneira temporal, e os achados devem ser construtivos, úteis para os jurisdicionados e significativos para todas as demais partes interessadas. O relatório deve ser submetido para as autoridades competentes conforme regimentalmente prevê a Corte de Contas.

## 1.6 ETAPAS DO RELATÓRIO

Dentre as etapas do estágio conclusivo do processo de auditoria cabe destacar a Formulação de Conclusões e Recomendações, as Limitações para Auditorias de TI e as Respostas ao Órgão (INTOSAI, 2013).

### 1.6.1 Formulação de Conclusões e Recomendações

Achados de Auditoria, conclusões e recomendações devem se basear em evidências. Ao formular a conclusão ou relatório de auditoria, o Auditor de TI deve atentar a materialidade do objeto no contexto da natureza da auditoria ou da entidade auditada (BRAZ, 2017).

O Analista devem emitir suas conclusões sobre os achados de auditoria baseados em objetivos previamente definidos. As conclusões devem ser relevantes, lógicas e imparciais. Conclusões generalistas a respeito da ausência de controles e riscos devem então ser evitadas. Recomendações quanto ao potencial para melhorias significativas das operações e seu desempenho devem ser emitidas baseadas em seus achados.

Analistas devem também relatar o status de achados significativos não corrigidos e recomendações de auditorias anteriores que afetem os objetivos da auditoria atual. Recomendações construtivas podem encorajar melhorias se endereçadas às partes competentes e levando em conta seus custos-benefícios.

### 1.6.2 Limitações para Auditorias de TI

As limitações para auditoria também devem ser apontadas em relatório. As limitações típicas podem ser o acesso inadequado a dados, ausência de documentação adequada de processo ou sistema, o que pode levar o Analista a adaptar seus métodos de investigação e análise para obter suas conclusões. Assim, qualquer limitação enfrentada deve ser apontada devidamente em relatório.

### 1.6.3 Respostas ao Órgão

Em se tratando de Relatórios de Auditorias de TI, é extremamente importante a obtenção de respostas das observações de auditoria. Auditores de TI devem planejar reuniões com o gerenciamento de alto nível do jurisdicionado e documentar suas respostas. Se esses esforços falharem, evidencias adequadas sobre os esforços empregados devem ser registradas e mencionadas em relatório.

# 2. GOVERNANÇA DE TI

A Governança de TI pode ser pensada como a estrutura geral que guia as operações de Tecnologia da Informação em uma organização com vistas a garantir o suprimento de suas necessidades atuais e futuras. É uma parte integrante da Governança Corporativa e engloba a liderança organizacional, estruturas e processos entre outros mecanismos (relatórios, feedbacks, coerção, recursos etc.) que garantem que a Infraestrutura de TI sustente os objetivos organizacionais gerenciando recursos enquanto mitiga os riscos de maneira efetiva (INTOSAI, 2013).

A Governança de TI desempenha um papel-chave na determinação do ambiente de controles e constrói a fundação para estabelecimento de práticas de controle interno por meio de fornecimento de relatórios de níveis funcionais para supervisão e revisão gerencial.

Existem vários padrões que definem os Princípios e Conceitos de Governança de TI e como uma organização pode escolher implantá-los.

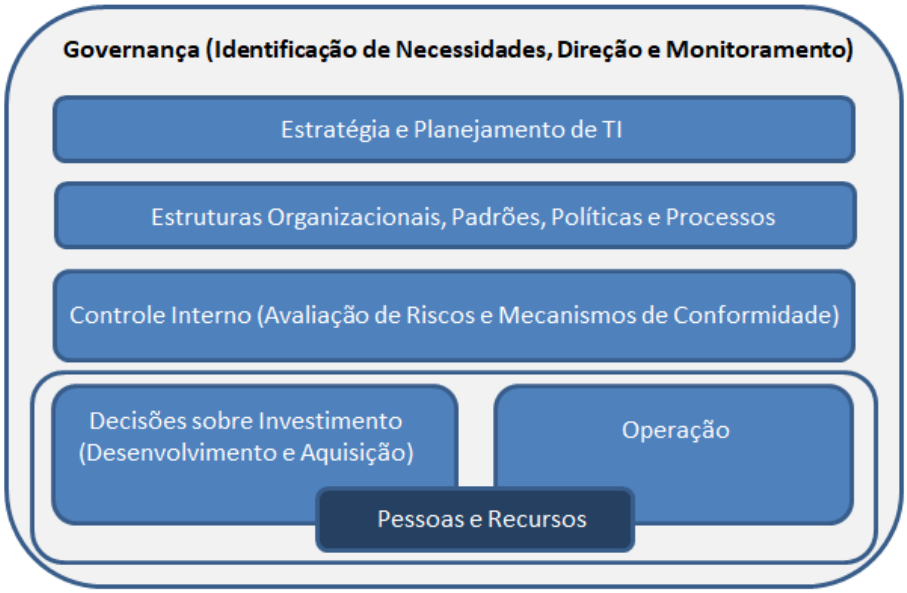


Figura 4 - Framework Genérico de Governança de TI

## 2.1 NECESSIDADES, DIREÇÃO E MONITORAMENTO

A Governança de TI é um componente-chave da Governança Corporativa. Ela pode ser definida na forma em que a TI agrega valor à Estratégia Geral de Governança Corporativa da organização. Ao adotar essa

abordagem, todas as partes interessadas são compelidas a participar do processo de tomada de decisão. Isso cria um senso geral de responsabilidade por sistemas críticos e garante que as decisões relacionadas a TI sejam tomadas e guiadas pelo negócio e não o contrário.

Para que a Governança de TI assegure que os investimentos em tecnologia agreguem valor ao negócio, e que os riscos associados a TI sejam mitigados, é essencial que a estrutura organizacional estabeleça papéis bem definidos de responsabilidade sobre a informação, processos de negócio, aplicações e infraestrutura. Também é essencial que a Governança de TI esteja envolvida na atualização ou identificação de novas as necessidades de negócio, e então ofereça as soluções apropriadas.

Durante o desenvolvimento e a aquisição da solução, a Governança de TI garante que a solução escolhida atenda ao negócio e que o treinamento e os recursos necessários (hardware, ferramentas, rede, capacidade, etc.) estejam disponíveis para sua implementação. O monitoramento das atividades deve ser desempenhado por grupos de controle interno ou garantia da qualidade, os quais devem periodicamente relatar seus resultados à gerência.

## 2.2 ELEMENTOS CHAVE PARA A GOVERNANÇA DE TI

Segundo o framework Cobit 5, as necessidades das partes interessadas dirigem o maior objetivo da governança: a criação de valor. Nesse sentido, o Cobit divide a criação de valor em três pilares (ISACA, 2018):

- Entrega de Benefícios;
- Otimização de riscos;
- Otimização de recursos.

Em resumo, quando a TI cria valor, ela está entregando benefícios por meio de uso otimizado dos recursos disponíveis em níveis aceitáveis de risco.

As necessidades das partes interessadas são influenciadas por diversos fatores, tais como o ambiente de negócios, as novas tecnologias, as demandas regulatórias, as mudanças de estratégia etc. Essas necessidades determinam os objetivos institucionais ou objetivos de negócio que, por sua vez, influenciam os objetivos de TI.

Visivelmente, a governança tem papel mais estratégico e está mais fortemente ligada à alta administração da organização. Objetivos, controles, estratégias e políticas são assuntos mais ligados à governança, enquanto a Gestão de TI tem aspecto mais tático e está mais voltada à administração dos recursos para consecução dos objetivos praticados.

Assim, conforme a norma NBR ISO/IEC 38500/2009, a Governança de Tecnologia da Informação compreende avaliar e direcionar o uso da TI para o suporte à organização e o monitoramento de seu uso com vistas à realização dos planos traçados. Essa norma define princípios da boa governança de TI que são (NASCIMENTO, 2010):

> *"**Responsabilidade**: Os indivíduos e grupos na organização devem compreender e aceitar as suas responsabilidades no fornecimento e na demanda de TI para, assim, garantir que a conduta ética da gestão para com o mercado, seus colaboradores, seus parceiros, na gestão financeira e fiscal.*
> ***Estratégia**: A estratégia de negócio da organização tem em conta as capacidades de TI atuais e futuras. Esta estratégia diz respeito ao como será realizada a abordagem da organização para o contexto de Governança.*
> ***Aquisições**: As aquisições de TI são feitas por razões válidas, com base e análise apropriada e continuada, com decisões claras e transparentes. Há um equilíbrio adequado entre os benefícios, oportunidades, custos e riscos, tanto no curto como no longo prazo.*
> ***Desempenho**: A TI é adequada à finalidade de suporte da organização, à disponibilização de serviços e quanto aos níveis e qualidade dos serviços necessários para responder aos requisitos do negócio. O desempenho precisa ser medido e monitorado através de metas e métricas que viabilizem a gestão avaliar os resultados que estão sendo obtidos e a tomada de ações corretivas necessárias a eficácia do processo de governança.*
> ***Conformidade**: A TI encontra-se em conformidade com a legislação e regulamentos aplicáveis, buscando uma postura transparente e adequada para com o mercado, a sociedade e a sustentabilidade.*
> ***Comportamento Humano**: As políticas, práticas e decisões na TI revela respeito pelo Comportamento Humano, incluindo as necessidades atuais e a evolução das necessidades de todas as "pessoas no processo. Enfatizando a importância das pessoas para que as mudanças necessárias adoção da Governança de TI sejam alcançadas."*

### 2.2.1 Planejamento e Estratégia de TI

A Estratégia de TI representa o alinhamento mútuo entre esta e os Objetivos Estratégicos Corporativos. Os Objetivos Estratégicos de TI devem considerar as necessidades atuais e futuras do negócio e a capacidade atual

da TI para a entrega de serviços. Deve considerar uma estrutura de TI existente assim como arquitetura, investimentos, modelo de entregas, recursos incluindo equipe e assim esboçar uma estratégia que integre esses elementos com vistas a apoiar os objetivos do negócio.

É importante que o Analista de Controle Externo revise a Estratégia da entidade com vistas a avaliar se sua abrangência parte do processo de tomada de decisão da organização (INTOSAI, 2013).

### 2.2.2 Estruturas organizacionais, padrões, políticas e processos

As Estruturas Organizacionais são um elemento-chave da governança de TI, principalmente no que tange a articulação de papéis de vários setores de administração e gerenciamento. Devem delegar de forma clara as responsabilidades para tomada de decisões e monitoramento. Estruturas organizacionais devem ser baseadas em padrões, políticas e procedimentos, visando aumentar a capacidade de tomada de decisões.

No setor público as estruturas organizacionais são influenciadas pelas Partes Interessadas, ou seja, grupos, organizações, membros, sistemas que afetem ou possam ser afetados pelas ações da organização como, por exemplo, a Assembleia Legislativa e o Cidadão. Estruturas organizacionais também são influenciadas pelos Usuários – internos e externos. Usuários internos são a alta direção da organização, departamentos que atuem em determinados processos de negócio e indivíduos da organização que interajam com estes. Usuários externos são demais órgãos, indivíduos que utilizem produtos ou serviços oferecidos pela organização. Outra influência nas Estruturas Organizacionais são os Fornecedores que podem se tratar de uma companhia, unidade ou pessoa, tanto externa quanto interna, que presta um serviço (NASCIMENTO, 2010).

Dessa forma sabemos que a necessidade de funcionalidades de TI surge dos usuários e das partes interessadas. Em todos os casos, o estabelecimento de estruturas organizacionais, papéis e responsabilidades são exigidas da alta direção do órgão e dela devem ter sua origem.

### 2.2.3 Funcionalidades da Estrutura Organizacional de TI

Comité Estratégico de TI – É uma peça central da estrutura organizacional. Ele inclui membros da alta cúpula, diretores e tem a responsabilidade na revisão, apoio e endereçamento de fundos para investimentos em TI. Decisões de investimentos que envolvam soluções “Desenvolver vs. Comprar” são de responsabilidade do Comitê Estratégico de TI, após as devidas recomendações equipes especializadas.

Finalmente, o comitê geral desempenha um papel crítico na promoção de aquisições e provê o suporte gerencial para programas que implementam mudanças na organização.

Em várias organizações do setor público, as funções do Comitê Geral de TI são partes da função gerencial (Secretaria dos Portos do Pará, 2016).

### 2.2.4 Padrões, Políticas e Processos

Padrões e políticas são adotados pela organização após aprovados pela alta direção. Políticas implementam procedimentos para as operações diárias visando atingir os objetivos definidos com base em procedimentos e processos que definem como trabalho será conduzido e controlado. Esses objetivos são definidos pela alta direção para cumprir a missão organizacional e, ao mesmo tempo estar em conformidade com as exigências legais e regulatórias. Políticas e procedimentos correspondentes precisam ser comunicados para todos os usuários relevantes da organização periodicamente (ISACA, 2012).

Algumas das políticas-chave que guiam a Governança de TI incluem:

#### 2.2.4.1 Política de Recursos Humanos

A Política de RH lida com a contratação, treinamento, direcionamento ao trabalho e outras funções da organização. Lida também com papeis e responsabilidades de várias equipes assim como as habilidades e treinamentos exigidos para suas atividades.

#### 2.2.4.2 Documentação e política de retenção

A documentação de sistemas da informação, aplicações, relatórios é uma referência importante para alinhar as operações de TI com os objetivos de negócio. Políticas de retenção de documentação apropriadas permitem o rastreamento e gerenciamento de mudanças em aplicações e infraestrutura de TI como um todo.

#### 2.2.4.3 Política de terceirização

A terceirização da TI é normalmente voltada a permitir que o gerenciamento do órgão concentre seus esforços nas suas atividades essenciais, pode ter origem também na necessidade de reduzir custos. Assim, uma política de terceirização deve garantir que a implementação da TI seja mais eficiente e econômica para organização.

#### 2.2.4.4 Política de Segurança de TI

Estabelece requisitos para proteção dos ativos de informação e procedimentos ou ferramentas que auxiliarão nessas atividades. A política deve estar disponível para todos os servidores da área de segurança da informação, incluindo usuários de sistemas de negócio que desempenhem salvaguarda de documentos (registros pessoais, dados financeiros, etc.).

## 2.3 CONTROLE INTERNO

O Controle Interno é o processo de introdução e implementação de um conjunto de medidas e procedimentos que determinem se as atividades da organização estão e permanecem consistentes com os planos aprovados. Se requeridas, medidas corretivas necessárias devem ser tomadas de maneira que os objetivos da política sejam alcançados (Portal de Auditoria, 2016).

As atividades de Controle Interno incluem o gerenciamento de riscos, a conformidade com procedimentos internos, instruções, legislações, regulamentos externos, relatórios de gerenciamento periódicos ou ad hoc. Consistem também na verificação de processos, revisão de planos e na realização de auditorias, avaliações e monitoramentos.

### 2.3.1 Gerenciamento de Riscos

O Gerenciamento de Riscos de TI deve ser parte integrante da estratégia e política gerencial da organização. Envolve a identificação dos riscos inerentes às aplicações existentes e à infraestrutura de TI. Dentre suas atividades estão gerenciamento contínuo de riscos, incluindo revisão periódica, atualização via estratégias de mitigação e monitoramento de riscos.

### 2.3.2 Mecanismos de Conformidade

As organizações devem estabelecer mecanismos de conformidade que garantam que todas as políticas e procedimentos associados estejam sendo seguidos. Basicamente é o fomento de uma cultura organizacional em que os empregados estejam sensíveis às não conformidades detectadas. Deve incluir o grupo de garantia da qualidade, uma equipe de segurança, ferramentas automatizadas e etc. Relatórios de não conformidade devem ser revistos pela gerência apropriada e problemas sérios ou repetitivos devem ser alvos de ação (INTOSAI, 2016).

O gerenciamento deve escolher lidar com as não conformidades por meio de treinamentos, mudanças de procedimentos ou ainda por procedimentos de retribuição.

Auditorias internas ou externas podem oferecer feedbacks periódicos sobre a conformidade da TI com as políticas organizacionais, padrões, procedimentos e objetivos gerais. Essas auditorias devem ser desempenhadas de maneira imparcial e objetiva oferecendo uma avaliação justa.

## 2.4 DECISÕES DE INVESTIMENTO

A governança de TI deve oferecer aos usuários de negócio soluções para suas necessidades seja pelo desenvolvimento de novo software ou adquirindo soluções de fornecedores, a depender do custo-benefício. Para atingir esse objetivo, as melhores práticas geralmente demandam uma abordagem disciplinada onde os requisitos são identificados, analisados, priorizados e aprovados, uma análise de custo-benefício conduzida entre soluções concorrentes e a melhor solução selecionada, que equilibre custo e riscos (ISACA, 2012).

## 2.5 OPERAÇÕES DE TI

Uma operação de TI é a execução cotidiana da infraestrutura tecnológica do órgão para apoiar as suas necessidades tornando possível a identificação de gargalos e o planejamento antecipado de mudanças em equipamentos, rede e sistemas, medindo a performance para manutenção da qualidade de serviço necessária. Deve prover um help-desk e o gerenciamento de incidentes para apoiar os usuários de recursos de TI (ISACA, 2012).

## 2.6 PESSOAS E RECURSOS

É recomendado que o gerenciamento avalie regularmente se os recursos alocados são suficientes para atingir as necessidades da organização, de acordo com as prioridades acordadas e as limitações orçamentárias, considerando as necessidades atuais e futuras das partes interessadas.

## 2.7 RISCOS PARA O ÓRGÃO AUDITADO

Os Analistas de Controle Externo precisam compreender e avaliar os diferentes componentes da estrutura de Governança de TI para promover direcionamentos, melhorias, suporte a decisões e o monitoramento das estratégias e objetivos da organização.

Para conduzir a avaliação o auditor precisa conhecer os componentes chave da Governança e o Gerenciamento da TI e estar ciente dos riscos associados à inadequação de cada componente da entidade.

Cada organização enfrenta seus próprios desafios e problemas de ambiente, políticos, geográficos e econômicos. Embora essa não seja uma lista exaustiva, as consequências apresentadas abaixo representam os riscos comuns e as consequências que podem resultar da falta de uma governança de TI apropriada (INTOSAI, 2013).

### 2.7.1 Infraestrutura de TI não efetiva, ineficiente ou não amigável

A Tecnologia da Informação na Administração Pública visa servir à sociedade e ampliar a atuação dos órgãos, e para tal soluções imensamente abrangentes e complexas se fazem necessárias. Essas soluções devem então ser devidamente projetadas, adaptadas as reais necessidades, coordenadas

com competência e executados de maneira eficiente. Uma governança de TI deficiente pode ser o primeiro obstáculo na obtenção de uma infraestrutura tecnológica adequada.

### 2.7.2 Estrutura de TI sem direcionamento

Pouco ou nenhum valor agregado pode ser obtido de investimentos em TI que não estejam estrategicamente alinhados com os objetivos organizacionais e seus recursos. Alinhamento estratégico deficitário significa que mesmo uma TI de boa qualidade pode não contribuir de maneira eficiente para o alcance dos objetivos gerais da organização. Uma maneira de garantir o alinhamento é envolver usuários e partes interessadas no processo de tomada de decisões.

### 2.7.3 Limitações ao Crescimento do Negócio

A falta ou a inadequação do planejamento pode gerar limitações ao crescimento da organização pela falta ou pelo uso ineficiente de recursos de TI. Uma forma de mitigar esse risco é a atualização periódica da estratégia de TI, que deve identificar recursos e planos para o alcance nas necessidades futuras da organização.

### 2.7.4 Gerenciamento Ineficiente de Recursos

Para alcançar bons resultados com poucos recursos, uma organização deve gerenciá-los de maneira eficiente, garantindo a disponibilidade de hardware, software e recursos humanos para a entrega de serviços de TI. Definir e monitorar o uso de recursos de TI, por exemplo, em um Acordo de Níveis de Serviço, permite à organização conhecer objetivamente se seus recursos requeridos são adequados para o alcance das necessidades do negócio.

### 2.7.5 Tomada de decisão inadequada

Uma estrutura de relatório deficitária pode ocasionar uma tomada de decisão inadequada, o que pode afetar às partes interessadas internas na entrega de seus serviços. Comitês Gerais e outros grupos organizacionais com

representação apropriada ajudam na tomada de decisões que afetem a organização.

### 2.7.6 Falhas de Projeto

Organizações por vezes falham ao avaliar a importância da Governança de TI. Isso ocorre especialmente quando são assumidos projetos sem compreensão das suas necessidades. Outra falha comum se dá quando as aplicações adquiridas ou desenvolvidas não cumprem com padrões mínimos de arquitetura e segurança, o que pode incorrer em custos adicionais para a Administração. A padronização de um ciclo de vida para desenvolvimento de sistemas é uma forma de reduzir os riscos de falhas de projeto.

### 2.7.7 Dependência de empresa terceirizada

A inexistência de um processo de controle de aquisições e de terceirização, pode levar a organização a enfrentar situações em que dependa completamente de fornecedor. Essa é uma situação de risco já que a saída de um fornecedor do mercado ou sua falha ao entregar os serviços contratados colocará a organização em uma situação difícil. Há também outros problemas, por exemplo, disputas sobre propriedade intelectual, sistemas e banco de dados. Organizações que terceirizam ou que contratam fornecedores regularmente devem ter políticas de aquisição e terceirização que definam o que pode ou não ser terceirizado.

### 2.7.8 Falta de transparência e prestação de contas

A prestação de contas e a transparência são dois importantes elementos da boa governança. Quando consistentemente aplicada, a transparência pode inibir a corrupção, melhorar a governança e promover a prestação de contas. Logo, na ausência de estruturas organizacionais, estratégias, procedimentos, controles de monitoramento adequados, a instituição pode falhar em sua regularidade e transparência.

### 2.7.9 Não conformidade com lei e regulamentos

A evolução dos controles sobre a Administração demandam garantias cada vez maiores de cumprimento a leis e regulamentos, assim como a atuação conforme as boas práticas de governança corporativa. Com a evolução da TI, há também uma necessidade crescente de garantia que contratos incluam requisitos importantes relacionados à privacidade, confidencialidade, propriedade intelectual e segurança. Devido às várias políticas que uma organização deve possuir, como Segurança de TI, Terceirização, Recursos Humanos, entre outras, é necessária a incorporação destas às suas estruturas legais e regulatórias.

### 2.7.10 Exposição aos Riscos de Segurança da Informação

Muitos riscos de segurança da informação podem surgir da ausência de estruturas apropriadas, processos e políticas, como: a apropriação indevida de ativos, informações confidenciais de acesso não autorizado, vulnerabilidade a ataques lógicos e físicos, indisponibilidade e ruptura de informações, mau uso da informação, não conformidade com leis e regulamentos sobre dados pessoais além de falhas na recuperação de desastres.

A Política de Segurança da Informação deve definir os ativos organizacionais (dados, equipamentos, processos de negócio) que precisam de proteção assim como procedimentos, ferramentas e controles de acesso físico que protejam tais ativos (INTOSAI, 2016).

A Governança de TI é então uma área chave das organizações do setor público. Isso faz com que os órgãos de controle devam inserir a Governança de TI como parte de suas Auditorias, o que pode contribuir com que a Tecnologia da Informação esteja na agenda geral da governança corporativa.

# 3. DESENVOLVER OU ADQUIRIR SISTEMAS

A Tecnologia da Informação oferece soluções com o objetivo de apoiar a estratégia de negócios. O processo de desenvolvimento, aquisição ou contratação de uma solução deve ser planejado de maneira que os riscos possam ser gerenciados e as chances de sucesso sejam maximizadas. Adicionalmente, os requisitos para a eficiência, efetividade e economicidade dessas soluções devem ser identificados, analisados, documentados e priorizados. As organizações devem também empregar testes e garantias de qualidade para assegurar a adequação dessas soluções.

Normalmente, soluções são desenvolvidas ou adquiridas por equipes de projeto. Embora algumas vezes as organizações não possuam a formalização de um projeto, ainda assim atividades precisam ser desempenhadas.

Conforme enuncia o Capability Maturity Model Integration for Aquisition (CMMI para Aquisição), versão 1.3 (Software Engineering Institute, 2010), as organizações estão cada vez mais se tornando adquirentes dado que produtos e serviços podem estar prontamente disponíveis e mais baratos que seu desenvolvimento interno. Contudo, os riscos na aquisição de produtos que não atinjam os objetivos do negócio ou falham ao satisfazer usuários é real e precisam ser gerenciados de maneira a atingir esses objetivos corporativos.

Quando feita de maneira disciplinada, a aquisição pode melhorar a eficiência operacional da organização ampliando a capacidade de fornecedores na entrega de soluções de qualidade, em custo baixo e com a tecnologia apropriada.

A aquisição de uma solução obviamente requer da organização um entendimento de suas necessidades e requisitos. O processo de identificação de requisitos deve envolver todas as partes interessadas no processo de negócio, incluindo usuários finais e equipe técnica, que podem necessitar eventualmente manter e prestar suporte ao sistema. Na aquisição de serviços (help desk, automação de desktop, etc,) a identificação de requisitos deve incluir o departamento de TI que será a interface da organização com o provedor de serviços. Requisitos devem ser postos em prioridade caso haja um

corte orçamentário ou restrições de custos, alguns podem ser adiados para futuras entregas ou aquisições conforme apropriado.

A definição dos requisitos é apenas um primeiro passo no processo de aquisição. A aquisição requer o gerenciamento de várias outras áreas, por exemplo, gerenciamento de riscos e programas, testes, supervisão de fornecedores tanto durante a aquisição quando em possível suporte ao sistema, treinamento interno, problemas de integração ou implementação.

## 3.1 ELEMENTOS-CHAVE DE DESENVOLVIMENTO E AQUISIÇÃO

Para balizar a escolha entre desenvolver ou adquirir uma solução, alguns elementos-chave devem ser levados em consideração (INTOSAI, 2013).

### 3.1.1 Requisitos de Desenvolvimento e Aquisição

Para qualquer desenvolvimento de projeto ou aquisição, a organização precisa documentar seus requisitos e gerenciá-los. Gerenciar requisitos inclui a priorizá-los adotando critérios como criticidade, custos e complexidade. Além dos proprietários de negócios, o processo de identificação de requisitos deve incluir usuários, equipe de apoio, experts em determinada área e outras partes interessadas quando apropriado.

Os requisitos formam, então, a base para tomada de decisão e devem, portanto, ser claros e concisos. Ao analisar e priorizar requisitos, a organização é capaz de avaliar custos e outras variáveis comerciais para chegar à solução ideal.

### 3.1.2 Controle e Gerenciamento de Projetos

O Gerenciamento de Projetos engloba planejamento e de atividades de controle. Inclui também a definições de custos, cronogramas e o envolvimento das partes interessadas em atividades-chave. O controle de projetos envolve a supervisão e fornecimento de relatórios periódicos para a tomada de ações corretivas quando o desempenho do projeto não segue o planejado. Por exemplo, se o custo do projeto aumenta substancialmente, a organização pode escolher cortar certas funcionalidades após consulta às partes interessadas (BRAZ, 2017).

A estrutura de gerenciamento de projetos deve ser descrita em uma abordagem de Ciclo de Vida ou ainda em uma Estratégia de Aquisição. O plano de projeto serve de base para guiar todas as atividades e reuniões periódicas com a alta direção devem ser realizadas para atualizações de status, gerenciamento de riscos e redirecionamento de recursos, agenda e etc., caso necessário.

### 3.1.3 Planejamento da Contratação

O início da etapa de planejamento é marcado pela elaboração de um Documento de Oficialização da Demanda (DOD). Nesse documento, a área requisitante deverá registrar as necessidades por uma solução de tecnologia, registrar a motivação para a contratação, efetuar a indicação de fontes de recursos e a indicação do integrante da área requisitante que, juntamente com o integrante da área técnica e o da área administrativa, formação a equipe de planejamento.

A partir do DOD, diversas atividades serão realizadas no âmbito do planejamento, iniciação, análise de viabilidade da contratação, análise de risco, elaboração do plano de sustentação e concepção da estratégia da contratação. Tais atividades são compostas por etapas fundamentais no processo de caracterização da solução que será contratada. A tabela abaixo sintetiza as etapas inerentes ao planejamento segundo (BRAZ, 2017).

| Etapa | Principais Atividades | Principais produtos gerados |
|---|---|---|
| Instituição de Equipe de Planejamento | Envio e análise do DOD à área administrativa; decidir motivadamente pela continuidade, instituir equipe de planejamento. | DOD validado<br>Equipe instituída. |
| Estudo Técnico Preliminar | Especificar requisitos; avaliar e comparar soluções; justificar solução escolhida; declarar viabilidade | Especificação de requisitos; comparação de soluções; avaliação de viabilidade. |
| Análise de riscos | Avaliar riscos; definir ações de contingência e responsáveis | Lista de riscos; análise de riscos e ações de mitigação. |
| TR ou Projeto Básico | Definição do objeto;<br>Justificativa e descrição da solução; responsabilidades da contratada; critérios de | PB ou TR |

| | | |
|---|---|---|
| | julgamento, orçamento, estimativa de impacto;<br>Consolidar informações dos artefatos;<br>Gerar projeto básico ou termo de referência | |

Tabela 1 - Etapas do Planejamento de Contratação

### 3.1.4 Seleção do Fornecedor

Uma vez executada a etapa de planejamento e tendo sido gerado o termo de referência ou projeto básico, inicia-se a etapa de seleção do fornecedor, a qual inaugura a fase externa da contratação. Os trâmites e procedimentos externos legalmente previstos serão desempenhados nessa etapa, que culmina na assinatura do contrato com o fornecedor selecionado.

A determinação da estratégia da contração, feita durante o planejamento, influenciará a condução da seleção do fornecedor, pois os meios necessários à realização da licitação foram definidos naquela etapa. De forma semelhante, em razão dos riscos à contratação presentes na etapa de seleção, a análise de riscos produzida anteriormente no planejamento terá papel importante. Muitos dos embates jurídicos e interrupções das contratações acontecem nessa fase, quando a competição é mais acirrada e os fornecedores adotam medidas com vistas a vencer o certame (Ministério do Planejamento, Desenvolvimento e Gestão, 2017).

Concluindo o certame, a assinatura do contrato encerra a etapa de seleção do fornecedor e será seguida pela destituição da equipe de planejamento e pela indicação dos gestores e fiscais do contrato.

| Etapa | Principais atividades | Principais produtos gerados |
|---|---|---|
| Avaliar Termo de Referência/Projeto Básico (TR/PB) e revisar tecnicamente. | Avaliar TR/PB e Revisar tecnicamente | TR/PB revisado |
| Preparar licitação | Confeccionar minuta de edital<br>Revisar recomendações técnicas e administrativas<br>Realizar audiência pública<br>Publicar instrumento convocatório | Edital de licitação<br>Instrumento convocatório publicado |
| Realizar licitação | Conduzir sessão pública<br>Responder | Fornecedor selecionado |

| | | |
|---|---|---|
| | questões/impugnações<br>Analisar propostas<br>Realizar habilitação<br>Adjudicar e homologar | |
| Etapas finais | Assinar contrato<br>Distituir equipe de planejamento, nomear gestor e fiscais | Contrato assinado, gestores e fiscais nomeados |

Tabela 2 - Etapas do Procedimento Licitatório

### 3.1.5 Garantia da Qualidade, Fiscalização e Testes

A equipe envolvida na Garantida da Qualidade/Fiscalização Contratual periodicamente avalia os produtos de trabalho visando o cumprimento dos padrões de qualidade acordados e a conformidade com os processos exigidos no desenvolvimento desses produtos. Os órgãos precisam verificar se a solução desenvolvida ou adquirida atende seus requisitos de aceitação e efetuar testes com o envolvimento das partes interessadas. A equipe de garantia da qualidade deve assegurar que a metodologia de desenvolvimento adotada esteja sendo seguida e que haja supervisão dos requisitos acordados. Por exemplo, as revisões (formais ou informais) devem ser conduzidas e relatórios de status necessários enviados para as partes interessadas. Além disso, a equipe de garantia da qualidade deve zelar pela adoção de políticas internas e procedimentos para aquisição ou esforços de desenvolvimento.

### 3.1.6 Gerência de Configuração

A Gerência de Configuração é utilizada para garantir que a integridade de documentos, software, outros descritivos e materiais de suporte sejam mantidos. Mudanças nesses materiais devem ser gerenciadas e controladas em versões, e estabelecidas de maneira que a organização seja capaz de voltar a uma versão anterior já testada. A equipe de Gerenciamento de Configuração também está envolvida na aprovação ou autorização de software para instalação no ambiente de produção. Geralmente isso é feito após testes de usuário e quaisquer testes adicionais necessários para garantir que outros sistemas continuem a operar.

## 3.2 RISCOS PARA A ENTIDADE AUDITADA

A contratação de empresa terceirizada não é em si uma estratégia equivocada. Recorrer à execução indireta é necessário para melhor aproveitamento das especialidades, para evitar o crescimento desmedido da máquina pública e para que seja possível concentrar-se nos aspectos prioritários do negócio institucional. No entanto, ‘o que’ e ‘como’ se terceiriza são aspectos que podem levar essa estratégia ao sucesso ou ao fracasso (BRAZ, 2017).

Dada a escassez de recursos humanos especializados em TI na Administração Pública, os gestores recorrem frequentemente à terceirização para o fornecimento de serviços. Ocorre que boa parte das instituições não está guarnecida por processos, pessoal e capacidade técnica para gerir a prestação desses serviços, o que, por vezes, faz com que o Analista de Controle Externo identifique setores de TI inteiramente dependentes de empresas contratadas sem a devida fiscalização por parte de servidor especializado o que conduz a uma série de problemas como:

- Dependência de fornecedores exclusivos;
- Contratações de TI dissociadas dos objetivos do negócio;
- Aplicações de TI falhando em atender os requisitos das unidades demandantes;
- Serviços de má qualidade;
- Remuneração de horas não produtivas;
- Conhecimento não absorvido e internalizado pela organização contratante;
- Terceirização ilegal, alocação indevida de mão de obra;
- Projetos mal sucedidos.

No desenvolvendo um software existem vários riscos e desafios que uma organização enfrenta para garantir o sucesso desse projeto. Riscos esses relacionados a habilidades em desenvolvimento, experiência em testes e gerenciamento de projetos, um custo razoável e benefícios estimados além da sua capacidade de monitorar e acompanhar o status do projeto.

A aprovação dos requisitos do software ou sistema deve incluir os usuários, os auditores devem verificar se estes são consultados para a

definição dos requisitos e ainda se a equipe de garantia da qualidade avalia objetivamente os sistemas em desenvolvimento. Como na aquisição, o gerenciamento demanda atualizações periódicas sobre a situação do projeto visando possíveis ações corretivas.

Diante de uma organização que adquire um sistema, o auditor deve determinar se há gerenciamento dos fornecedores e obtenção de relatórios periódicos de status e se as devidas ações corretivas são tomadas. Para isso, o contrato deve especificar marcos de desenvolvimento onde haja revisões formais e relatórios que informem o órgão sobre custos, cronograma e desempenho. O auditor deve garantir que o gerenciamento da organização ou pessoal designado esteja recebendo, revisando e tomando ações corretivas com base em relatórios periódicos e atividades de contrato sempre que necessário.

# 4. OPERAÇÕES DE TI

Operações de TI são geralmente descritas como “as tarefas diárias que envolvem a execução, o suporte de sistemas da informação de uma organização (servidores em execução, manutenção, armazenamento adequado, serviço de helpdesk, etc.)”. A efetividade operacional das operações são medidas e gerenciadas usando Indicadores de Desempenho para Operações-chave de TI (KPIs) e a maioria das organizações documentam esses dados em forma de um acordo entre os usuários do negócio e a TI da organização. O Acordo de Nível de Serviços (SLA) é um acordo formal, onde esses parâmetros e outras decisões são documentados (INTOSAI, 2013).

## 4.1 ELEMENTOS-CHAVE DAS OPERAÇÕES DE TI

Algumas áreas ou elementos das operações de TI que o auditor precisará analisar para determinar se o órgão está efetivamente gerenciando as Operações de TI incluem, Projeto de Serviços e Entregas, Gerenciamento de Capacidade e Serviço, Procedimento para Resolução de Incidentes com vistas a assegurar a continuidade das operações e práticas envolvidas no gerenciamento de mudanças. Essas e outras áreas são definidas no ITIL (AXELOS, 2017), um dos frameworks mais adotados na identificação, planejamento, entrega e suporte a serviços de TI.

Para determinar se a entidade auditada está efetivamente entregando os serviços documentados o Analista deve avaliar o SLA, que deve estabelecer parâmetros específicos para vários serviços.

## 4.2 GERENCIAMENTO DE SERVIÇO E CONTINUIDADE DE TI

O Gerenciamento de Continuidade visa à manutenção dos requisitos contínuos da organização. O Departamento de TI atinge esse objetivo ao estabelecer metas de tempo de recuperação para componentes de TI que apoiem os processos de negócio, baseando-se em necessidades e requisitos acordados (INTOSAI, 2013). Ainda, a gerência de continuidade inclui revisões periódicas e atualização dos tempos de recuperação para garantir que seja

mantido o alinhamento com o Plano de Continuidade de Negócios e suas prioridades.

## 4.3 GERENCIAMENTO DE SEGURANÇA DA INFORMAÇÃO

O Gerenciamento da Segurança da Informação está relacionado aos riscos que envolvam a segurança, a tomada de ações e a garantia de que a informação esteja disponível, útil e completa quando necessário. Também está relacionado à garantia de que somente usuários autorizados tenham acesso às informações e que a transferência destas esteja protegida.

## 4.4 GERENCIAMENTO DE INCIDENTES E PROBLEMAS

O Gerenciamento de Incidentes são os sistemas e práticas utilizados para determinar ser incidentes ou erros são registrados, analisados e resolvidos em uma periodicidade adequada. O Gerenciamento de Problemas visa a resolução de questões por meio de investigação e análise de incidentes maiores ou recorrentes de maneira a identificar a causa raiz. Uma vez identificado o problema e conduzida à análise de sua causa raiz, ele se torna um erro conhecido ou ineficiência, então uma solução pode ser desenvolvida para trata-lo, evitando ocorrências futuras e incidentes relacionados.

Um mecanismo deve ser estabelecido para a detecção de falhas e para documentação das condições que identifiquem sua ocorrência. A equipe de operações de TI deve documentar procedimentos para detecção e registro dessas condições. Exemplos de incidentes podem incluir tanto acesso por usuários não autorizado, falhas na rede, baixa funcionalidade de software ou falta de capacitação de usuários.

## 4.5 GERENCIAMENTO DE MUDANÇAS

Nas Organizações de TI, o processo de gerenciamento de mudanças é normalmente utilizado para gerir e controlar ativos, como softwares, hardwares e documentações relacionadas. Controles de mudanças são necessários para garantia de que toda mudança sejam autorizada, testada, documentada e controlada de maneira que os sistemas continuem a apoiar as operações de negócio conforme planejado e com uma adequada rastreabilidade.

Mudanças acidentais ou não aprovadas podem levar a riscos e prejuízos para uma organização. Estas devem seguir um procedimento de gerenciamento de mudanças definido e aprovado pela direção antes da implementação no ambiente operacional. O processo de gerenciamento de mudanças deve garantir registros, avaliações, autorizações, priorizações, testes, implementações, documentações e revisões de acordo com os procedimentos documentados e aprovados de gerenciamento de mudança.

Mudanças podem iniciar, por exemplo, no modelo de negócio, nas necessidades operacionais ou pelo resultado de análises de incidentes/problemas. O Controle de Mudança deve incluir procedimentos para gerenciamento de autorização, gerenciamento de revisão nos efeitos de qualquer mudança, manutenção de registros adequados, preparação de planos de retroatividade (caso algo inesperado aconteça) e o estabelecimento de procedimentos para mudanças emergenciais.

O custo da mudança, o impacto nos sistemas de TI e objetivos de negócio, o efeito de sua não implementação, os requisitos futuros de recursos, variáveis determinantes na autorização e mudanças de prioridade devem ser considerados.

Mudanças emergenciais não podem aguardar para seguir os procedimentos de mudanças normais, e devem ser implementadas dentro de um prazo mínimo. Há tempo reduzido para implementar e testar tais mudanças. Isso cria um risco maior de erros e falhas de programação.

Onde existirem procedimentos de mudanças emergenciais, o auditor deve checar se eles são razoáveis e incluir alguma forma de controle. Isso pode incluir aprovação de mudanças emergenciais por um membro da equipe com a competência apropriada, aplicando controle de versão e com trilha para auditoria (uso de aplicações de controle de mudança apropriadas), aprovação retroativa do gestor de mudanças/responsável pelo sistema, testes retroativos e atualização de documentação.

## 4.6 ACORDO DE NÍVEL DE SERVIÇO

Os Acordos de Nível de Serviço documentam vários parâmetros que o Departamento de TI utiliza para oferecer serviços para o negócio. Os

parâmetros na SLA são geralmente acordados pelas partes interessadas e a equipe de TI. O auditor deve utilizar esses parâmetros para averiguar se os níveis de serviço estão sendo atingidos, se as partes interessadas estão satisfeitas e tomando as ações apropriadas em caso de desvio desses parâmetros (Ministério do Planejamento, Desenvolvimento e Gestão, 2017).

A SLA contém, entre outros itens, Indicadores Desempenho para os serviços de TI. Revisar esses indicadores auxiliará o auditor a formular questionamentos relacionados à:

- Operabilidade dos sistemas conforme os acordos estabelecidos
- Estabelecimento de Mecanismos para avaliação de desempenho e identificação de ações corretivas dela decorrentes.
- Avaliação de controles auxiliando abrangência de testes.

Exemplos de medições por Indicadores de Desempenho e definições e metas:

| **Processo** | **Meta (Fator Crítico de Sucesso)** | **Indicador chave de performance** | **Arquitetura de Medição** |
|---|---|---|---|
| Gerenciamento de Mudança | Redução de incidentes causados por mudanças não autorizadas | Redução percentual em número de incidentes resultantes de acesso não autorizado | Gerenciamento de Incidentes, Mudanças de Configuração registradas e reportadas mensalmente. |

Tabela 3 - Indicadores de Desempenho

Podem existir casos em que a organização terceirizou o núcleo de suas funções para um fornecedor. Nesses casos, a organização é responsável pela gestão do fornecedor de modo a garantir que as necessidades de negócio estejam sendo atendidas.

## 4.7 RISCOS PARA A ENTIDADE AUDITADA

A ferramenta principal para o auditor, como dito anteriormente, é o Acordo de Níveis de Serviço. Ele oferece os parâmetros, indicadores de desempenho e requisitos os quais a organização deve avaliada. Se esse documento possui lacunas, não sofreu revisão formal ou aprovação pelas

partes interessadas, há um risco de que os recursos de TI da organização possam não estar sendo utilizados da maneira mais eficiente e efetiva. Ao auditar operações de TI, é necessário o acesso ao documento onde os objetivos gerais e os parâmetros técnicos estejam definidos, o que constitui, normalmente, o SLA.

Na área de Gerenciamento de Mudanças, o auditor deve avaliar se há procedimentos para as mudanças estabelecidas no sentido de dar a garantia da integridade do sistema e que apenas aplicações testadas e aprovadas sejam introduzidas no ambiente operacional.

O auditor deve também se preocupar em como a organização está gerenciando sua capacidade (armazenamento, CPU, recursos de rede e etc.) de maneira proativa para atendimento aos usuários, gerenciamento de incidentes e outras questões de segurança de forma que as funções do negócio não sejam comprometidas.

# 5. TERCEIRIZAÇÃO

Terceirização é a substituição de um processo de negócio interno ou aquisição de uma nova função de negócio, por meio da contratação de uma entidade externa. A Entidade Contratada é responsável por oferecer os serviços exigidos contratualmente em troca de pagamento (BRAZ, 2017).

A esse respeito o Decreto-Lei 200/1967 dispõe:

> *"Art. 10. A execução das atividades da Administração Federal deverá ser amplamente descentralizada.*
>
> *§ 7º Para melhor desincumbir-se das tarefas de planejamento, coordenação, supervisão e controle e com o objetivo de impedir o crescimento desmesurado da máquina administrativa, a Administração procurará desobrigar-se da realização material de tarefas executivas, recorrendo, sempre que possível, à execução indireta, mediante contrato, desde que exista, na área, iniciativa privada suficientemente desenvolvida e capacitada a desempenhar os encargos de execução."*

Com base nesse artigo podemos inferir que as tarefas de planejamento, coordenação, supervisão e controle são próprias da administração pública, cuja execução deve ser priorizada em detrimento de tarefas executivas e operacionais.

A organização pode escolher terceirizar partes selecionadas ou toda sua infraestrutura, serviços ou processos de TI com base em uma política. Dependendo da criticidade do serviço terceirizado, a organização pode optar pela implementação de controles mais ou menos formais sobre o serviço. As organizações devem decidir se terceirizam toda ou algumas de suas operações visando:

1. Flexibilização da Equipe: A terceirização permite a otimização de recursos em caso de demandas cíclicas ou sazonais, ou seja, recursos que ficam periodicamente ociosos.
2. Desenvolvimento da Equipe: Se um projeto requer habilidades que a organização ainda não possui, ela pode decidir terceirizar seu projeto ao invés de treinar a equipe interna, poupando tempo e custos em treinamento. Assim, ao utilizar o expertise técnico e as locações físicas de fornecedores, a organização pode alocar uma equipe para trabalhar ao lado do fornecedor e assim promover treinamento prático para sua equipe.
3. Redução de custos: A terceirização pode deslocar os custos de mão de obra para o fornecedor, que normalmente gasta

> menos com pessoal. A organização deve priorizar a terceirização de atividades que seriam mais custosas se mantidas internamente. Um exemplo seria a operação de algum sistema que requeira treinamento. Terceirizar operações não essenciais também auxilia o foco da organização na promoção da eficiência em sua atividade-fim.
> 4. A terceirização permite que a organização conte com o auxílio de especialistas em questões relativas a atividades existentes ou emergentes. A entidade torna-se capaz de responder rapidamente a necessidades de mudança nos negócios com a ajuda especializada.

De acordo com (ISACA, 2012), entidades podem terceirizar várias áreas de negócio e infraestrutura de TI. Por exemplo:

- Infraestrutura operacional como data center e processos relacionados.
- Processamento de aplicações internas em um provedor de serviços.
- Sistemas de desenvolvimento ou manutenção de aplicações.
- Instalação, manutenção e gerenciamento de computadores e redes associadas.

Um avanço recente em questões de terceirização é a utilização do que vem a ser conhecido como Computação na Nuvem. Nesse caso a organização terceiriza o processamento de dados para computadores pertencentes a um fornecedor. Essencialmente o fornecedor cede o equipamento, enquanto a entidade auditada ainda tem controle sobre as aplicações e os dados. A terceirização pode também incluir a utilização de máquinas do fornecedor para armazenamento, backup e provimento de acesso online para os dados da organização.

## 5.1 ELEMENTOS-CHAVE DA TERCEIRIZAÇÃO

Analisaremos os elementos-chave para uma terceirização que garanta eficácia e economicidade para uma organização (INTOSAI, 2013).

### 5.1.1 Política de Terceirização

Organizações precisam de uma política que defina que funções podem ser terceirizadas e quais funções devem permanecer internas. Geralmente as

organizações terceirizam operações de TI rotineiras, como manutenção ou mesmo plataformas de hardware. Informações de RH geralmente são mantidas internamente, pois demandam monitoramento mais próximo e estão sujeitas a várias exigências de privacidade e segurança que podem não agregar custo-benefício à terceirização.

O Analista deve avaliar a política e os procedimentos de terceirização da entidade auditada. Em entidades maiores, que frequentemente tem uma grande fatia de suas operações terceirizadas, é essencial uma política de terceirização aprovadas incluindo processos de solicitação claramente estabelecidos. Organizações menores podem não possuir uma política formal, mas devem seguir procedimentos de solicitação transparentes e eficientes.

### 5.1.2 Solicitação

Solicitação é o processo de documentação de requisições e a combinação de outras referências materiais que auxiliarão o fornecedor provimento do serviço. Isso inclui a geração de um pacote de solicitação para apresentação, obtenção de propostas e seleção entre vários fornecedores. O processo de seleção deve ser transparente e objetivo, baseado em critérios adequados para os sistemas ou serviços a ser adquiridos (Ministério do Planejamento, Desenvolvimento e Gestão, 2017).

### 5.1.3 Gerenciamento de Contrato / Fornecedor

O gerenciamento de contratação é um elemento-chave na terceirização para que os serviços sejam realizados de acordo com a expectativa do cliente. A entidade auditada deve ter processos estabelecidos para acompanhamento periódico dos status do projeto, fiscalização de serviço, e testes prévios a sua introdução no ambiente operacional. Ainda, como parte do processo de monitoramento, a entidade auditada deve também fiscalizar a qualidade interna do fornecedor para garantir que a equipe empregada esteja seguindo políticas aprovadas contratualmente.

O auditor deve observar se o órgão realiza Estudos Técnicos Preliminares antes da seleção do fornecedor e garante que os requisitos específicos e operacionais estejam presentes no contrato e na SLA por meio

de fiscalização do contratado. Ainda, deve ser auditado se o órgão tomou atitudes quando o fornecedor não atingiu o estipulado no acordo.

### 5.1.4 Acordos de Nível de Serviço (SLA)

O Acordo de Nível de Serviço é um acordo documentado entre a organização e o fornecedor e é uma ferramenta-chave na gestão serviços contratados. O SLA deve definir os serviços cuja realização é esperada assim como os parâmetros técnicos para estes, vinculando o fornecedor à organização.

As áreas cobertas por SLA são, comumente (Ministério do Planejamento, Desenvolvimento e Gestão, 2017):

- Tipos de serviço implementados pelo fornecedor.
- Definição de responsabilidades entre a organização e o fornecedor.
- Medição de serviços, que inclui: período de medição, duração, localidade, e cronograma de relatórios (taxa de defeitos, tempo de resposta, horas de help-desk, etc.).
- Tempo para implementação de nova funcionalidade, níveis de retrabalho.
- Tipo de documentação exigida para aplicações desenvolvidas pelo fornecedor.
- Localização onde os serviços serão realizados.
- Frequência de back-up, parâmetros de recuperação de dados.
- Prazos e formatos e métodos de entrega de informações.
- Cláusulas de incentivo e penalidades.

Em resumo, a maioria dos itens que são críticos para a organização devem ser colocados em Acordos de Nível de Serviço. O Analista de Controle Externo deve avaliar o SLA ou outro documento (acordo formal ou contrato) onde esses parâmetros estejam documentados para garantir que o informado pelo fornecedor esteja atingindo os requisitos e que a organização tenha tomado ações corretivas relacionadas a deficiências.

### 5.1.5 Valor agregado à Organização

Além da redução de custos há outros benefícios que não são diretamente mensuráveis, como o aproveitamento da infraestrutura do fornecedor para ampliação do serviço ou o uso de seu expertise em situações especiais. Sempre que possível o órgão deve determinar de maneira periódica se as economias projetadas estão sendo alcançadas. Isso serve como um dos marcos para decidir continuar ou não com a terceirização.

## 5.2 RISCOS PARA O JURISDICIONADO

A terceirização de um processo de seu negócio implica ao jurisdicionado uma série de riscos, que devem, portanto, ser mitigados.

### 5.2.1 Retenção de Conhecimento e Propriedade do Processo

Há um risco inerente de perda de conhecimento organizacional, que normalmente transita entre os desenvolvedores e as aplicações. Se o fornecedor, por algum motivo, deixa de prover o serviço, os órgãos devem estar prontos para reassumir a tarefa. Ainda, se o desenvolvimento de uma aplicação se der de maneira terceirizada, há também o risco de perda da propriedade do processo de negócio, que pode ser reivindicado pelo provedor de serviço seu. Os órgãos precisam enfrentar essa questão no momento da redação contratual e assegurar a obtenção da documentação completa da solução provida, como, por exemplo, diagramas de projeto do sistema evitando dependência do fornecedor.

### 5.2.2 Falha na entrega por parte de fornecedor

Por vezes um fornecedor pode falhar na entrega de uma solução, seja quanto ao prazo ou quanto à funcionalidade acordada. Se o processo de solicitação não foi implementado corretamente há uma alta probabilidade de o sistema ou serviço adquirido não atender as necessidades dos usuários, ter qualidade inferior, custar mais, requerer recursos significativos para manutenção/operação ou ser de baixa qualidade a ponto de ter que ser substituído em um futuro próximo. Um contrato mal redigido, uma falha na

seleção do fornecedor, etapas de entrega mal definidas ou condições de mercado desfavoráveis são algumas das razões mais comuns de fracasso do fornecedor.

Os órgãos precisam ter planos de contingência para quando isso acontecer. Quando a terceirização for considerada, as organizações devem avaliar as implicações de uma falha do fornecedor para o negócio. Disponibilidade de documentação detalhada quanto ao projeto de serviços ou sistemas auxiliará a organização na garantia de sua continuidade.

### 5.2.3 Desvios de Escopo

Todos os contratos terceirizados contêm premissas e presunções. Se a atividade atual destoa das estimativas, o cliente pagará a diferença. Esse fato tem se tornado um grande obstáculo para as organizações que acabam sendo surpreendidas por um preço não fixado ou mudanças adicionais de escopo. A maior parte dos projetos varia entre 10-15% em termos de especificações durante o ciclo de desenvolvimento (INTOSAI, 2013).

### 5.2.4 Aproveitamento de membros-chave da equipe

O crescimento de fornecedores de serviços criou uma nova dinâmica no mercado de trabalho. Profissionais capacitados estão frequentemente à procura de projetos novos, especializados e que aumentem sua perspectiva financeira. Assim, uma estatística importante a ser gerenciada é a volatilidade da equipe. Taxas de volatilidade normalmente estão entre 15 e 20% e a criação de termos contratuais em torno desses níveis é uma requisição razoável (INTOSAI, 2013).

### 5.2.5 Riscos Externos

A contratação de serviços de outros países é uma forma comum de terceirização, especialmente na utilização de ambientes de Computação na Nuvem. Nesse cenário, os riscos dessa terceirização devem envolver regulamentação estrangeira em armazenamento e transferência de informações e pode limitar o que pode ser armazenado e como isso será processado, dados podem ser utilizados por demanda legal de um país

estrangeiro sem o conhecimento da organização, padrões de privacidade e segurança podem ser desproporcionais e diferentes jurisdições podem ser necessárias para solução de conflitos.

# 6. PLANO DE CONTINUIDADE DE NEGÓCIOS E PLANO DE RECUPERAÇÃO DE DESASTRES

As organizações governamentais confiam cada vez mais na disponibilidade e na correta operação de seus sistemas da informação, esses, por sua vez, desempenham papeis importantes em diversas atividades.

Quedas de energia, ações industriais, incêndios, ações maliciosas podem ocasionar efeitos desastrosos na estrutura de TI, podendo levar várias semanas para a retomada das suas operações caso não haja um Plano de Continuidade de Negócios efetivo.

Os termos Plano de Continuidade de Negócios (BCP) e Plano de Recuperação de Desastres (DRP) são muitas vezes utilizados como sinônimos, mas na verdade constituem dois termos complementares. Ambos são importantes para o Analista de Controle Externo, pois juntos eles garantem que a organização seja capaz de se manter operacional após a ocorrência de falhas (INTOSAI, 2016). Consistem em:

- Plano de Continuidade de Negócios (BCP) é o planejamento e teste da recuperação de seus processos de negócio após uma ocorrência. Ele também descreve como uma organização continua a funcionar sob condições adversas, como desastres naturais ou de outra ordem.
- Plano de Recuperação de Desastres (DRP) é o planejamento para recuperação da infraestrutura de tecnologia da informação após um desastre natural ou de outra ordem. É um subconjunto do Plano de Continuidade de Negócios. O BCP se aplica as funções organizacionais de negócio e o DRP atua sob os recursos de TI que apoiam as funções de negócio.

Na essência, o BCP é voltado para a manutenção da capacidade organizacional quando as operações normais estão comprometidas. Esse plano inclui políticas, procedimentos e práticas que permitem à organização recuperar e retomar processos críticos após um desastre ou crise.

Além de declarar as práticas que devem ser seguidas na ocorrência de uma interrupção, os BCP incluem outros componentes como recuperação de desastres, resposta a emergência, recuperação de usuário, contingência e atividades de gerenciamento de crise. Assim, nessas organizações, a continuidade do negócio é vista como um termo que abrange tanto a recuperação de desastres como a retomada das atividades do negócio.

Entretanto, seja parte do BCP ou em um documento separado, as DRPs devem definir recursos, ações, tarefas e os dados necessários para gerir a recuperação da organização comprometida. Esse plano deve também auxiliar na restauração dos processos de negócio afetados, destacando os passos específicos que a companhia deve seguir em seu caminho. Especificamente, a DRP é usada para o planejamento e preparação para minimizar os danos ocasionados e garantindo a disponibilidade dos sistemas de informação críticos da organização. Em termos de TI, DRP é voltada para a recuperação de bens tecnológicos críticos, incluindo sistemas, aplicações, bancos de dados, dispositivos de armazenamento entre outros recursos de rede.

## 6.1 ELEMENTOS-CHAVE DO BCP E DO DRP

O Analista de Controle Externo deve avaliar os programas de gerenciamento de continuidade da entidade, a avaliação de sua recuperação a desastres, planos de continuidade de negócio e sistemas de gerenciamento de crise. Para isso, é preciso compreender em que consiste a estratégia de gerenciamento de continuidade do negócio e os passos seguidos para avaliação da efetividade dos programas existentes.

Um planejamento de continuidade efetivo possui várias fases (BRAZ, 2017):

- Política e Plano de Continuidade do Negócio
- Função de Continuidade de Negócio da Organização
- Avaliação de Impacto ao Negócio (BIA) e Gerenciamento de Risco
- Controles Preventivos incluindo controles de ambiente
- Plano de Recuperação de Desastre
- Documentação do Plano de Continuidade do Negócio

- Teste e treinamento do Plano
- Segurança durante a implementação do BCP/DRP
- Backup e recuperação de desastres para serviços terceirizados.

Esses passos representam elementos chave em um planejamento de continuidade de negócio abrangente.

### 6.1.1 Política e Plano de Continuidade de Negócio

Um plano de continuidade efetivo começa com o estabelecimento de uma Política de Continuidade de Negócio. A equipe de gerenciamento de continuidade, representando todas as demais funções apropriadas, desempenha um papel importante para o sucesso da continuidade organizacional. A declaração da política de planejamento de continuidade de negócios deve definir os objetivos gerais da organização e estabelecer uma estrutura e responsabilidades para o planejamento de continuidade.

### 6.1.2 Estabelecimento da Função de Continuidade do Negócio

Para ser bem-sucedido, a equipe de gerenciamento de continuidade do negócio deve se organizar em termos de representar todas as funções de negócio apropriadas. A alta gerência e outras partes interessadas devem apoiar o programa de continuidade bem como o desenvolvimento de sua política. Papeis e responsabilidades da equipe devem estar claramente identificados e definidos.

### 6.1.3 Avaliação de Impacto de Negócio e Gerenciamento de Riscos

Um avaliação de impacto de negócio e gerenciamento de riscos efetiva se dá em diversas etapas.

### 6.1.4 Avaliação de criticidade das operações e identificação de recursos

Em toda organização, a continuidade de certas operações é mais importante que outras, de forma que não é produtivo oferecer o mesmo nível de continuidade a todas as operações. Por isso, é importante que as

organizações determinem quais atividades são as mais críticas e quais recursos são necessários para recuperá-las e auxiliá-las. Isso se dá por meio de uma avaliação de riscos, na identificação de prováveis ameaças e seus impactos na informação e recursos relacionados da organização incluindo dados, softwares e operações de aplicação. O risco e avaliação de impacto deve abranger todas as áreas funcionais. As decisões quanto a riscos residuais devem ser devidamente tomadas onde o impacto de uma possível ameaça é mínimo ou os controles de sistema são adequados para destacar essas ocorrências oportunamente.

#### 6.1.4.1 Identificação e priorização das informações e operações críticas

A criticidade e a sensibilidade de várias informações e operações devem ser determinadas e priorizadas baseadas em categorias de segurança por meio de avaliações gerais de risco das operações. Essa avaliação de risco deve servir como base para um plano de segurança organizacional. Fatores a serem considerados incluem a importância e a sensibilidade da informação e de outros ativos organizacionais assim como o custo da não restauração de dados ou operações prontamente. Por exemplo, uma interrupção de um dia de sistemas de coletas impostos ou multas, a perda dessas informações pode diminuir drasticamente as receitas e reduzir a confiabilidade perante o público. Já um sistema de monitoramento do treinamento de empregados pode ficar inoperante por talvez vários meses sem consequências graves.

#### 6.1.4.2 Estabelecendo Prioridades de Processamentos de Emergência

Em conjunto com a identificação e o ranking de funções críticas, a organização deve desenvolver um plano para restaurar essas operações. O plano deve identificar de forma clara a ordem em que vários aspectos do processo devem ser restaurados, quem é o responsável, que equipamento de apoio ou outros recursos podem ser necessários. Um plano de restauração de processo cuidadosamente desenvolvido pode auxiliar os empregados a começar a restauração imediatamente, e fazer um uso mais eficiente dos recursos computacionais durante uma emergência. Tanto usuários de sistemas

e equipe de suporte em segurança da informação devem estar envolvidas na determinação das prioridades de processamento emergenciais.

#### 6.1.4.3 Prevenção e minimização de danos potenciais e interrupções

Há vários passos que a organização deve seguir para evitar ou minimizar os danos para suas operações automatizadas:

- Duplicação ou backup periódico de arquivos, programas e documentos críticos com armazenamento exterior ou estabelecimento localidades para backup remoto que podem ser usados caso o espaço físico da entidade esteja danificado.
- Estabelecimento de um sistema de recuperação e reconstituição de informação de maneira que os sistemas da informação possam ser recuperados e reconstituídos após uma falha ou interrupção.
- Instalação de controles de ambiente, como sistemas de extinção de fogo ou geradores de energia elétrica.
- Garantia de que a equipe e outros usuários de sistema compreendam suas responsabilidades na ocorrência de emergências.

Manutenção efetiva de hardware, gerenciamento de ocorrências e gerenciamento de mudanças.

#### 6.1.4.4 Implementação de Procedimentos de Backup

A cópia periódica de dados e sistemas, além dos seus armazenamentos em uma localização remota e segura são normalmente as ações mais produtivas que a organização pode tomar para mitigar as interrupções desses serviços. Embora um equipamento possa ser prontamente substituído, o custo pode ser significativo e a reconstituição de arquivos, assim como a substituição de softwares pode ser extremamente dispendiosa em custos e em tempo. Ainda assim, alguns dados podem não ser reconstituídos. Além do custo direto da reconstituição de arquivos e obtenção de software, interrupções de serviço relacionados podem levar a perdas financeiras significativas.

#### 6.1.4.5 Treinamento

A equipe deve ser treinada e estar ciente de suas responsabilidades na prevenção, mitigação e resposta a situações de emergência. Por exemplo, a equipe de suporte em segurança da informação deve receber treinamento periódico em incêndios, inundações e procedimentos em situações excepcionais, assim como em suas responsabilidades na inicialização e execução de procedimentos alternativos de retomada operacional. Também, se usuários externos são críticos para as operações da organização, eles devem ser informados dos passos a seguir nessas situações.

#### 6.1.4.6 Gerenciamento de Manutenção, Problemas e de Mudanças

Interrupções inesperadas de serviços podem ocorrer por falhas em equipamentos ou por mudanças sem a notificação antecipada aos usuários. Para evitar essas ocorrências um efetivo programa de manutenção é exigido, este é composto, principalmente, por (INTOSAI, 2013):

a. *Controles preventivos e de ambiente*: Evitam ou mitigam danos potenciais em equipamentos e interrupções no serviço. Controles de ambiente podem diminuir as perdas causadas por algumas interrupções como incêndios ou evitar incidentes por meio da detecção antecipada de potenciais problemas, como vazamentos de água ou fumaça, de forma que eles possam ser remediados. Também, geradores de energia podem manter os equipamentos em funcionamento durante quedas ou oferecer um período para backup de dados em conjunto com procedimentos de desligamento ordenado durante longos períodos sem energia. Exemplos de controles de ambiente incluem:
    i. Sistemas se supressão de fogo
    ii. Alarmes de incêndio
    iii. Detectores de fumaça
    iv. Detectores de água
    v. Iluminação de emergência
    vi. Redundância em sistemas de refrigeração de ar
    vii. Geradores de energia elétrica
    viii. Existência de válvulas de desligamento e procedimentos para linhas de encanamento que possam danificar equipamentos.
    ix. Equipamentos construídos com materiais resistentes ao fogo e projetados para reduzir a sua disseminação
    x. Políticas que proíbam alimentos, bebidas e cigarros em áreas com equipamentos.
b. *Plano de Recuperação de Desastres:* deve ser desenvolvido para a restauração de aplicações críticas. Ele inclui medidas para processamento alternativo de informações em caso de danos significativos ou inacessibilidade de equipamentos ou sistemas. Políticas e procedimentos de nível organizacional definem o processo e documentos de planejamento da recuperação. Além disso, um plano organizacional deve identificar os sistemas críticos, aplicações e quaisquer planos subordinados ou relacionados. É importante que esses planos sejam claramente documentados, comunicados para a equipe

pertinente e atualizado para refletir as operações atuais. devem ser documentados com a adesão dos departamentos de negócio e de segurança da informação além de comunicado à equipe afetada. O plano deve refletir as prioridades de risco e operacionais que a entidade identificou. Ele deve ser projetado de forma que os custos do planejamento de recuperação não excedam os custos associados com os riscos que o planejamento está destinado a reduzir. O plano deve ser detalhado e documentado de forma suficiente para que seu sucesso não dependa do conhecimento ou expertise de um ou dois indivíduos.

c. *Localidades Alternativas:* Dependendo do grau de continuidade de serviço necessário, as escolhas de localidades alternativas vão abranger desde um estabelecimento pronto para serviço imediato de backup, conhecido como um “hot site”, a um site que tomará algum tempo em preparação das operações, chamado de “cold site”. Além disso, vários tipos de serviços podem ser pré-combinados com fornecedores. Isso inclui o acordo com fornecedores de um hardware computacional e serviços de telecomunicação, bem como um fornecedor de formulários de negócio e outros suprimentos.
d. *Testes periódicos:* Testar o Plano de Continuidade é essencial para lidar com situações de emergência. Os testes podem revelar fraquezas importantes como instalações de backup que não repliquem operações críticas conforme antecipado. Por meio de procedimentos de teste, esses planos devem ser substancialmente melhorados. A frequência dos testes do plano de continuidade varia dependendo da criticidade das operações da organização. Normalmente os planos de continuidade para funções críticas devem ser testados integralmente ao menos uma vez a cada um ou dois anos, sempre que mudanças significativas no plano tenham sido tomadas ou quando ocorrer troca de pessoas chave da equipe. É importante para a alta administração avaliar problemas no plano de continuidade, e desenvolver uma política que abranja a frequência e a extensão desses testes. Resultados de testes de continuidades oferecem uma medida importante da viabilidade do plano de continuidade. Assim, eles devem ser reportados a alta gestão de maneira que a necessidade de modificação e testes adicionais possam ser determinadas e que a alta administração esteja ciente dos riscos das operações de continuidade advindos de um planejamento inadequado.
e. *Segurança:* A segurança de recursos e operações deve ser inclusa nos planos de continuidade do negócio como dados críticos. Aplicações, operações e recursos tendem a ser comprometidos facilmente durante a ocorrência de desastres ou atividades de gerenciamento de continuidade de negócios. Por exemplo, durante um procedimento de backup de dados, a falta de segurança pode acarretar à criação de cópias e vazamentos de dados importantes.
f. *Backup e recuperação de dados em serviços terceirizados:* Várias organizações terceirizam toda ou parte de suas atividades para um provedor de serviços. Sendo os controles e as operações rotineiras executados por terceiros, é essencial a garantia de que a continuidade dos negócios e o plano de recuperação de desastres esteja previsto em contrato. A organização deve também monitorar a implementação da continuidade de negócios e a prontidão do processo de recuperação de desastres oferecidos pelo provedor de serviços. Isso também inclui exigências de segurança para o provedor de serviços, como a confidencialidade dos dados e aplicações mantidos. Já a propriedade dos processos de negócio deve ser mantida pela organização que deve também se planejar para caso haja mudança de provedor de serviço.

## 6.2 RISCOS PARA A ENTIDADE AUDITADA

Produtos ou serviços críticos são os que devem ser entregues para garantir a sobrevivência, evitar perdas e cumprir exigências legais ou outras obrigações de uma organização. BCP/DRP é um processo de planejamento proativo que garante que os processos de negócio e a infraestrutura de TI de uma organização sejam capazes de apoiar as necessidades organizacionais após um desastre ou uma interrupção. Órgãos Públicos possuem várias atividades importantes (pagamentos, acesso a saúde, educação, segurança e outros serviços com os quais conta o cidadão). Se esses serviços forem interrompidos por um longo período, podem ocorrer perdas de várias ordens, incluindo financeiras. Auditores devem garantir que os órgãos do governo tenham processos BCP/DRP que garantam que o órgão seja capaz de oferecer continuidade aos serviços ao cidadão.

Ao avaliar se os processos de BCP/DRP são capazes de garantir e proteger a confiabilidade e continuidade da infraestrutura de TI há alguns riscos de auditoria que devem ser analisados durante a avaliação da efetividade de um plano de continuidade de negócios e recuperação de desastres. Eles devem cobrir todas as áreas funcionais críticas. Se a recuperação de desastres de uma área funcional está comprometida, a continuidade dos processos será deficiente. Se os papéis e as responsabilidades não são claros e absorvidos pela equipe envolvida um plano de continuidade pode não ser efetivo.

A avaliação de impacto no negócio, controles preventivos e de ambiente, documentação, testes e treinamento de pessoal apoiam a implementação efetiva do plano de continuidade de negócios da organização. Segurança deficiente na implementação do plano de continuidade e de recuperação de desastres possuem um risco de perda de dados e tempo valioso, além de outros custos devido a recuperação indevida em caso de desastres.

Serviços terceirizados apresentam uma área de riscos distintos onde o BCP e o DRP não estão em controle total da organização. Há riscos de segurança, perda, uso não autorizado e vazamento de informações que necessitam ser enfrentados.

# 7. SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação pode ser definida como a capacidade de uma organização de proteger dados e recursos com respeito à autenticidade, confidencialidade e integridade. A proteção da informação e de sistemas envolve medidas contra acesso não autorizado, modificação indevida de informações seja no armazenamento, processamento ou tráfego além de garantias contra a negação de serviços para usuários autorizados, e também a segurança de equipamentos e das comunicações.

A segurança da informação deve garantir a disponibilidade, confidencialidade e integridade, no qual toda a organização depende, se tornando um portal dos ativos de TI da organização. Isso demanda a proteção dos dados e infraestrutura organizacionais, permitindo à organização a busca de seus objetivos organizacionais sob um nível aceitável de risco. Oferecer informação aos que dela dependem é tão importante quanto protegê-la contra acesso não autorizado (BRAZ, 2017).

## 7.1 A NECESSIDADE DE SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação é cada vez mais importante para as instituições governamentais já que a interconexão entre redes públicas e privadas assim como o compartilhamento de recursos aumenta a complexidade do controle de acesso, assim como a necessidade de preservação de confidencialidade, integridade e disponibilidade dos dados.

Sistemas da Informação são a reunião de tecnologias complexas, processos e pessoas que colaboram para gerenciar o processamento, armazenamento e transmissão de informação para apoiar a missão e funções do negócio é essencial que cada organização construa seu programa de segurança da informação.

O objetivo de um programa de segurança de sistemas da informação é proteger a informação da organização reduzindo o risco de perda de confiabilidade, integridade, disponibilidade de dados em um nível aceitável. Sem segurança da informação a organização terá que lidar com riscos e

potenciais ameaças para sua operação e para o alcance dos objetivos gerais o que afetará sua credibilidade.

Enquanto cresce a complexidade e o papel da tecnologia da informação, a segurança se torna um tópico cada vez mais importante em Auditorias de TI sendo um fator crítico nas atividades organizacionais podendo acarretar danos em áreas como (INTOSAI, 2013):

- Lei – Violação de requisitos legais e regulatórios
- Reputação – Danos à reputação organizacional, quebra na confiabilidade perante outras organizações ou até dano à imagem do governo ou unidade da federação.
- Finanças – multas, desperdício de recursos.
- Produtividade – Redução da efetividade e eficiência em um projeto ou serviço ofertado pela organização.
- Vulnerabilidade – Dados e sistemas acessados de maneira não-autorizada propiciam o ingresso de softwares maliciosos que podem abrir caminho para invasões.

Danos esses que podem ser causados por:

- Falhas de segurança
- Acesso não autorizado a sites externos
- Exposição da informação – divulgação de bens organizacionais e informações sensíveis

## 7.2 FORMAÇÃO DA CULTURA DE SEGURANÇA DA INFORMAÇÃO

Um fator determinante para o sucesso dos programas de segurança da informação em uma organização é a criação de uma cultura organizacional que envolva essa área. Para lidar de maneira uniforme com essas questões um modelo organizacional de segurança da informação deve ser seguido. Os elementos envolvem:

- Criar uma consciência de segurança: Consiste em sessões educacionais para os colaboradores para começar a introduzir as responsabilidades de segurança da informação. A função de recursos humanos deve ser responsável pelo treinamento inicial

de novos empregados. Os treinamentos devem abranger desde o ingresso de um novo colaborador até seu desligamento.

- Busca de comprometimento da gerência: É um atributo único na formação da cultura de segurança da informação. Não se dá somente na preparação de uma documentação formal em políticas de segurança, mas também em se manter ativamente envolvida. Se a gerência não apoia genuinamente o programa de segurança da informação, ela pode desencorajar o senso de obrigação e responsabilidade dos colaboradores.
- Construir coordenações sólidas estabelecendo equipes multidisciplinares posto que a segurança da informação envolve vários aspectos da organização, o que encoraja a comunicação e a colaboração além de reduzir o isolamento departamental e o retrabalho.

O estabelecimento de uma Cultura de Segurança da Informação é uma parte integrante da implementação de uma Governança de TI, e se caracteriza por:

- Alinhamento da Segurança da Informação e Objetivos de Negócio: Demanda controles de segurança da informação para oferecer uma redução de riscos real e mensurável.
- Avaliação de Riscos: Determina a forma de controles necessários. A aplicação de uma avaliação de riscos auxilia na seleção de controles apropriados para mitigar os riscos de maneira efetiva.

O processo de avaliação de riscos inclui a identificação e a análise de:

- Processos e ativos relacionados a sistemas
- Potenciais ameaças que podem afetar a confidencialidade, integridade ou disponibilidade de sistemas.
- Vulnerabilidades de sistema e ameaças associadas
- Potenciais impactos e riscos oriundos de ameaças
- Exigências de proteção para a efetiva mitigação de riscos.

- Seleção de medidas de segurança apropriadas e análise de relações de risco.

Equilíbrio entre organização, pessoas, processos e tecnologia: A Segurança da Informação efetiva requer apoio organizacional, profissionais competentes, processos eficientes e seleção de tecnologias apropriadas. Cada elemento interage com outro de diferentes áreas, impactos e apoia outros elementos, por vezes de maneira complexa de forma que é crucial o equilíbrio entre eles. Se algum desses elementos é deficiente, a segurança da informação é enfraquecida.

## 7.3 ELEMENTOS-CHAVE DA SEGURANÇA DA INFORMAÇÃO

Existem elementos que são primordiais para o estabelecimento de uma Segurança da Informação efetiva no âmbito organizacional (BRAZ, 2017).

### 7.3.1 Ambiente de Segurança da Informação

Para apoiar a implementação bem-sucedida da Segurança da Informação, existem alguns elementos fundamentais que devem ser alcançados:

- Confidencialidade: É a preservação de restrições de acesso à informação e divulgação, incluindo meios para proteção da privacidade e da propriedade. Para sua constante manutenção, o sistema deve assegurar que cada indivíduo controle qual informação é coletada sobre ele, como ela é utilizada, quem a utilizou, quem a mantém, e para qual propósito ela é utilizada.
- Integridade: É a proteção contra modificação ou destruição imprópria da informação, o que inclui a garantia de não repúdio e autenticidade. Para se certificar a integridade da informação um mecanismo de autenticidade é necessário garantindo que os usuários sejam as pessoas que dizem ser.
- Disponibilidade: É assegurar que todos os sistemas da informação incluindo hardwares, redes de comunicação, aplicações e os dados que estes armazenam estejam disponíveis

para usuários nos momentos necessários para realização das suas atividades no negócio. Entretanto, esse acesso deve ser submetido a uma política de controle que assegure que os usuários somente acessem os recursos e serviços que lhe sejam cabíveis e que não seja negado o acesso a quem tenha legitimidade para tal.

A Segurança da Informação trata também de minimizar a exposição, baseando-se no gerenciamento de riscos. Uma falha ao implementar e monitorar um processo de mitigação de riscos em uma área pode causar danos a toda a organização. Mesmo sendo de amplo conhecimento que o gerenciamento efetivo de riscos de segurança é essencial para a organização, esses riscos são por vezes negligenciados ou as precauções de segurança não são atualizadas em resposta a mudanças.

### 7.3.2 Avaliação de Riscos

Como já exposto anteriormente, a avaliação de riscos é o processo de identificação e análise da infraestrutura de segurança em TI envolve o levantamento desde ameaças internas e externas de uma entidade até seus ativos e seu pessoal.

### 7.3.3 Política de Segurança

A política de segurança da organização é um conjunto de leis, regras e práticas que regulam como a organização gerencia, projeta e distribui recursos para alcançar objetivos específicos de segurança. Essas leis, regras e práticas devem identificar critérios para atribuição de autoridades individuais e deve especificar condições sob as quais aos indivíduos é permitido o exercício desta autoridade. Uma forma recomendada de Política de Segurança em TI é a seguinte:

| **Elementos de uma Política de Segurança em TI** |
|---|
| Definição de Segurança da Informação – Objetivos e Escopo |
| Princípios de segurança, padrões e requisitos de conformidade detalhados |
| Definição de responsabilidades gerais e específicas para todos os aspectos de segurança da informação. |
| Uso de ativos de informação e acesso a e-mail, Internet, entre outros |
| Modo e método de acesso |

| |
|---|
| Procedimentos de backup |
| Procedimentos para lidar com softwares maliciosos |
| Elementos de educação e treinamento em segurança |
| Processo para relatos de suspeitas de incidentes em segurança |
| Planos de continuidade de negócio |
| Métodos de comunicação para a equipe política e procedimentos adotados para segurança da informação. |

**Tabela 4 - Elementos de uma Política de Segurança em TI**

### 7.3.4 Organização da Segurança de TI

A organização da segurança da TI implica implementar a política de segurança na entidade. Esse trabalho pode ser atribuído a uma unidade ou indivíduo que trabalha com a TI da organização para aquisição de ferramentas apropriadas e implantação de processos para uma efetiva política de segurança. Eles são também responsáveis por oferecer o treinamento para a equipe e por tratar os incidentes de segurança.

Há também uma necessidade em assegurar proteção adequada aos dados acessados ou transferidos a organizações externas. O analista precisará averiguar se a entidade é capaz de implementar os requisitos de segurança da informação como documentado.

### 7.3.5 Gerenciamento de Ativos

Refere-se ao monitoramento e manutenção de bens que possuem valor para a organização por meio da operação, manutenção, atualização e disposição de ativos de maneira eficiente.

Para a tecnologia da informação, gerenciamento de ativos inclui manter um inventário atualizado do equipamento e TI, conhecer que licenças associadas aos equipamentos, manutenção e proteção de equipamento (bloqueios, salas controladas, etc). O Gerenciamento de Ativos de TI também inclui o gerenciamento de documentações de software e processos que tenham valor para a organização.

Para uma entidade governamental, o gerenciamento de ativos de TI é muito importante no ambiente fiscal atual, pois restrições financeiras podem não permitir a reposição de ativos perdidos ou furtados de uma maneira razoável. Além disso, a organização pode estar em risco se não possuir um

inventário completo de seus ativos quando necessária a atualização de software em futuras necessidades da organização.

### 7.3.6 Segurança de Recursos Humanos

Empregados que lidam com dados pessoais em uma organização precisam receber o treinamento de conscientização adequado assim como atualizações regulares em um esforço para salvaguardar os dados que lhes são confiados. Papéis e responsabilidades apropriadas atribuídas para cada descrição de trabalho precisam ser definidos e documentados em alinhamento com a política de segurança. Os dados do órgão devem ser protegidos de acessos não autorizados, divulgação, modificação, destruição ou interferência. O gerenciamento de segurança de recursos humanos é necessário durante todas as fazes do ciclo de vida de um colaborador.

As três áreas dos Recursos Humanos são:

- Pré-contratação: Definir papéis e responsabilidades para a atividade, definir o acesso apropriado a informações sensíveis, determinar a profundidade dos níveis de acesso, de acordo com a política de segurança de TI. Durante essa fase, os termos contratuais devem também ser estabelecidos.
- Durante a contratação: Empregados com acesso a informações sensíveis em uma organização devem receber lembretes periódicos de suas responsabilidades e receber atualizações frequentes por meios de treinamentos de conscientização para garantir seu entendimento das ameaças atuais e práticas de segurança correspondentes para mitigar tais ameaças.
- Término ou mudança contratual: Para evitar acesso não-autorizado a informações sensíveis, o acesso deve ser revogado imediatamente no momento do término/mudança contratual de um empregado. Isso inclui também a devolução de quaisquer ativos da organização que estiverem com ele.

Um programa de sensibilidade em segurança deve ser estabelecido com o intuito de lembrar toda a equipe de possíveis riscos além de suas responsabilidades perante as informações corporativas.

### 7.3.7 Segurança Física e de Ambiente

A segurança física descreve medidas previstas para negar acesso físico não autorizado a um prédio, instalação, recurso ou informação armazenada assim como a orientação em como projetar estruturas para resistir a potenciais atos hostis. A segurança física pode ser simples como uma porta trancada ou elaborada como várias barreiras, guardas armados ou instalação de guaritas (INTOSAI, 2013).

A segurança física a princípio se preocupa com a restrição ao acesso físico a pessoas não autorizadas a instalações controladas, embora existam outras considerações e situações nas quais medidas de segurança física sejam importantes como prevenção de incêndios e enchentes.

Segurança inevitavelmente implica em custos e nunca é perfeita ou completa. Em outras palavras, segurança pode reduzir riscos, porém não pode eliminá-los inteiramente. Uma segurança física robusta aplica combinações de controles sobrepostos e complementares. Por exemplo, controles de acesso físico para instalações protegidas são geralmente propostos para:

- Desencorajar potenciais intrusos (ex. sinais de alerta e marcas de perímetro).
- Distinguir pessoas autorizadas das não autorizadas (ex. uso de crachás e chaves).
- Retardar, frustrar e evitar tentativas de intrusão (ex. paredes fortes, fechaduras de portas e cofres).
- Detectar invasões e monitorar intrusos (ex. alarmes e sistema interno de TV).
- Disparar as respostas a incidentes apropriadas (ex. por guardas ou polícia).

#### 7.3.7.1 Controle de Acesso

O Controle de Acesso se refere a elencar quem é autorizado a interagir com determinado recurso e envolve uma autoridade responsável por esse controle. O recurso pode ser um prédio, grupo de prédios ou sistemas de TI. Controle de Acesso é, seja físico ou lógico, um fenômeno cotidiano. Uma fechadura em uma porta de um carro é uma forma simples de controle de acesso. Uma senha em um caixa eletrônico é outra forma assim como dispositivos biométricos. A limitação exercida por meio de controle de acesso é de suma importância quando pessoas procuram proteger informações e equipamentos importantes e confidenciais (WETHERALL & TANENBAUM, 2011).

Em um ambiente governamental várias entidades processam dados de forma que preocupações com a privacidade devem limitar quem manipula essas informações. O controle de acesso assegura que somente usuários com as credenciais adequadas tenham acesso para tal informação.

#### 7.3.7.2 Aquisição, desenvolvimento e manutenção de Sistemas

O Ciclo de Vida de Desenvolvimento de Sistemas (SDLC), Processo de Desenvolvimento de Software ou Engenharia de Software, é um processo de criação e alteração de sistemas da informação, e modelos e metodologias são usados para o desenvolvimento desses sistemas. Na engenharia de software, o conceito SDLC abrange vários tipos de metodologias de desenvolvimento de software. Essas metodologias formam um framework para planejamento e controle da criação de um sistema ou do processo de desenvolvimento de software.

A manutenção de um sistema inclui mudanças e atualizações como resultado de novos requisitos, resolução de erros e melhorias feitas como resultado de novas interfaces.

#### 7.3.7.3 Gerenciamento de Incidentes de Segurança de TI

No campo da Segurança em TI, o gerenciamento envolve a monitoração e detecção de eventos de segurança em um computador ou rede, e a execução das respostas apropriadas a esses eventos. O gerenciamento de

incidentes de segurança em TI é a forma especializada e gerenciamento de incidentes.

#### 7.3.7.4 Gerenciamento de Continuidade de Negócios

O planejamento de continuidade de negócios é o conjunto de ações por meio das quais uma organização testa a recuperação de seus processos após uma interrupção. Ele também descreve como uma organização continua a funcionar em condições adversas (por exemplo, desastres naturais).

#### 7.3.7.5 Conformidade

O auditor de TI deve revisar e avaliar a conformidade de todos os requisitos internos e externos (legais, ambientais, qualidade da informação, confiabilidade e segurança).

## 7.4 RISCOS PARA A ENTIDADE AUDITADA

Uma Política de Segurança em TI permite que a organização proteja sua infraestrutura de usuários não autorizados. Ela estabelece requisitos de alto nível para a organização e seus empregados para salvaguardar ativos críticos. Ela também oferece direcionamento à equipe garantindo que todos sigam procedimentos estabelecidos para acesso e controle de dados. Ainda, a política de TI faz referência a leis e outros regulamentos que a organização deve seguir. Existem vários obstáculos que a organização enfrenta ao implementar um sistema de segurança da informação. Sem a governança efetiva para lidar com esses obstáculos, a segurança de TI poderá não atingir os objetivos da organização.

Cada organização enfrenta desafios únicos posto que seus ambientes, políticas, geografias, economias e questões sociais diferem, apresentando obstáculos para oferecer a efetiva governança de TI. Assim, é responsabilidade do auditor apontar riscos de segurança da informação para a gerência.

Estes são os riscos mais significativos identificados na maioria das organizações (INTOSAI, 2013):

- Divulgação não autorizada de informação.
- Modificação ou destruição não autorizada de informação.

- Vulnerabilidade a ataques a sistemas.
- Destruição de infraestrutura de sistemas.
- Interrupção de acesso, uso da informação ou sistema da informação.
- Interrupção de processamento de sistema da informação.
- Roubo de dados.

No que tange a exposição a riscos para organizações auditadas, uma atenção especial deve ser dada as áreas:

- Estratégias de Segurança da Informação não alinhadas com os requisitos de TI ou de negócios.
- Políticas não aplicadas uniformemente com imposições variadas
- Não conformidade com requisitos internos e externos
- Segurança da Informação não inclusa em processos de manutenção de portfólio e de desenvolvimento.
- Arquitetura resultando em soluções de segurança da informação não efetivas, ineficientes ou equivocadas.
- Medidas inadequadas de segurança física e gerenciamento de ativos.
- Configuração inadequada de hardwares.
- Organização ineficiente de processos de sistemas da informação e estrutura de responsabilidades de sistemas.
- Soluções de recursos humanos inadequadas.
- Uso ineficiente de recursos financeiros em segurança da informação, custo-benefício da segurança da informação não alinhado com as necessidades no negócio.

Segurança da Informação não monitorada ou monitorada de maneira ineficiente.

O Analista deve começar por avaliar a adequação dos métodos de avaliação de riscos e levar em consideração questões de auditoria relacionadas à implementação de segurança da informação. Uma matriz de

auditoria auxiliará no levantamento dessas questões, critérios para avaliação, documentos.

Por fim, o analista deve desenvolver um programa de auditoria detalhado de acordo com as necessidades e o desenvolvimento durante auditoria em campo.

# 8. CONTROLES DE APLICAÇÃO

Aplicação é um tipo de software utilizado para realizar e apoiar processos de negócio. Pode incluir procedimentos manuais ou automatizados para produção de transações, processamento de dados, armazenamento e preparo de relatórios. Cada entidade provavelmente terá um número de aplicações em execução, que abrange desde sistemas corporativos acessados por todos os empregados até pequenas aplicações acessadas por apenas um.

A revisão de controles de aplicação permite que o auditor ofereça à organização uma avaliação independente da eficiência e efetividade do projeto além da operacionalidade dos controles internos e procedimentos relacionados à automatização de processos de negócio e identificação de questões relacionadas à aplicação que requeiram atenção (INTOSAI, 2013).

Visto que controles de aplicação estão intimamente relacionados a transações individuais, é mais fácil verificar como o teste de controles proporcionará ao auditor a garantia da precisão de uma funcionalidade. Por exemplo, testar controles em uma aplicação de folha de pagamento oferecerá a garantia do valor gasto com pessoal de um determinado órgão.

Dependendo dos objetivos de auditoria, a revisão da aplicação pode ter diferentes abordagens, assim, os controles avaliados variam de uma auditoria para outra. Por exemplo, a auditoria de uma aplicação pode se focar em conformidade com a lei e padrões, de forma que deva ser verificada a presença de controles de aplicação tratando essas questões. De outra perspectiva, a auditoria pode fazer parte de uma auditoria operacional, assim é importante averiguar como as regras de negócio estão traduzidas na aplicação. Durante uma análise de segurança da informação, o foco deve ser nos controles de aplicação responsáveis por garantir a confidencialidade, integridade e disponibilidade de dados.

Os passos a serem realizados na avaliação de controles de aplicação devem envolver um procedimento cíclico de atividades. Embora possa ser interessante começar da perspectiva do negócio, é importante notar que não há hierarquia estrita entre esses passos.

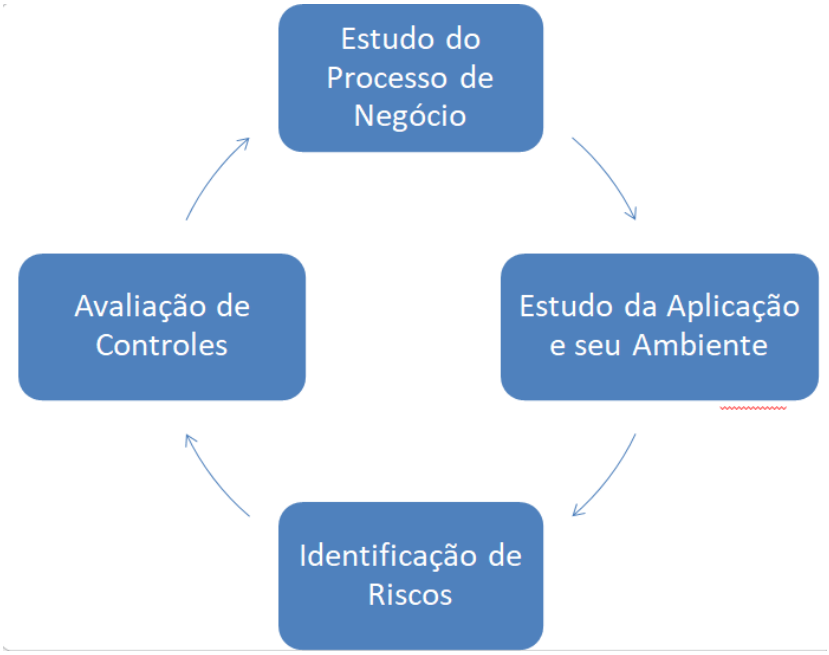


Figura 5 - Ciclo de Avaliação de Controles de Aplicação

Alguns deles são listados abaixo e brevemente descritos nas seções seguintes:

- Estudo do processo de negócio: Antes de explorar questões técnicas, pode ser útil obter um panorama sobre os processos de negócio automatizados pela aplicação, tais como regras, fluxos, atores, papéis e requisitos de conformidade relacionados. A compreensão das regras de negócio é um passo importante para a verificação da consistência dos controles e dos processos automatizados. A extensão desse passo varia de acordo com o objetivo da auditoria. Ele geralmente é feito por meio do estudo dos procedimentos operacionais, gráficos de fluxo de processos da organização ou outro material de referência. A equipe de auditoria pode também requerer entrevistas com gerentes de negócio, executivos de TI e usuários da aplicação.
- Estudo da aplicação e seu ambiente: Estudar o projeto e o comportamento da aplicação seja pela revisão da documentação (diagramas da organização, diagramas de fluxo de dados, manuais de usuário) ou entrevista com peças-chave. Estudar as funções do software em campo pela observação e interação com

equipe operacional durante o trabalho também é essencial. Por meio de discussões, deve se realizar um passo-a-passo dos processos de negócio e da aplicação desde a entrada de dados até a exibição de resultados. Verificar o fluxo real do processo e observar atividades manuais que podem ensejar controles complementares. Conversar com gerentes, operadores e desenvolvedores para obtenção de documentação em infraestrutura técnica: sistema operacional, ambiente de rede, sistema de gerenciamento de banco de dados, interface com outras aplicações, processamento de transações em lote, tempo real ou online. Isso dá uma indicação de como a infraestrutura de tecnologia impacta a aplicação.

- Identificação de Riscos: É essencialmente identificar riscos associados à atividade/função de negócio apoiado por uma aplicação e verificar como esses riscos são tratados. Algumas vezes a avaliação de riscos de um processo de negócio pode estar disponível (caso tenha sido feita outra auditoria) e o analista pode se beneficiar de sua utilização após avaliar a confiabilidade da avaliação existente de riscos.
- Avaliação de Controles: Após estar ciente do ambiente (de negócios e técnico) em torno da aplicação, o auditor deve avaliar os controles utilizados para tratar os riscos existentes. O analista deve ser cuidadoso ao sugerir melhorias. Por exemplo, detalhes excessivos em logs de transação podem acrescentar sobrecarga de custos e podem não indicar as informações desejadas. A avaliação deve envolver diferentes tipos de controles de aplicação que estão descritos na seção seguinte.

## 8.1 ELEMENTOS-CHAVE DE CONTROLES DE APLICAÇÃO

Enquanto Controles Gerais de TI estabelecem o tom de todo o ambiente tecnológico, os controles de aplicação são desenvolvidos para softwares específicos com o intuito de garantir e proteger a precisão, integridade, confiabilidade e confidencialidade da informação. Eles garantem

que as transações sejam devidamente autorizadas, dados válidos de entrada sejam processados e completamente registrados.

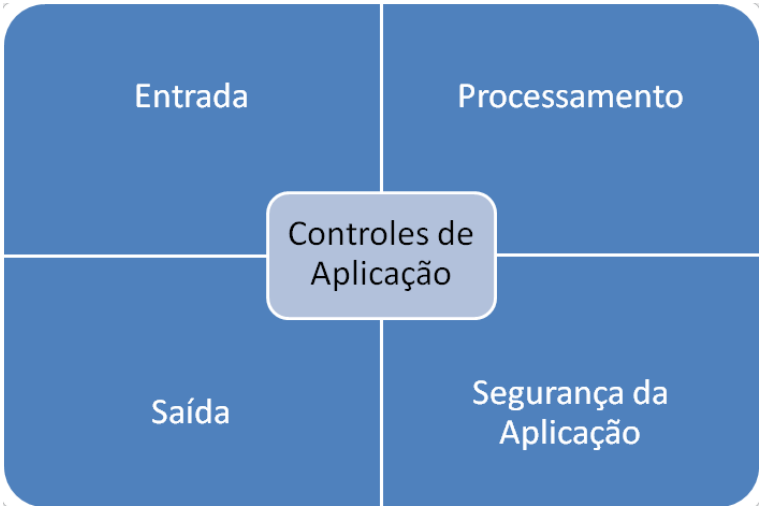


Figura 6 - Elementos-chave de controle de aplicação

Controles de Aplicação também incluem procedimentos manuais que operam em proximidade com a aplicação. Esses controles não são somente implementados em aplicações específicas, mas em todo o processo de negócio que o circunda. Por exemplo, um operador pode requerer que um dado de entrada seja assinado antes de ser inserido em um sistema.

A combinação de controles manuais e automáticos é por vezes um resultado de considerações sobre custos e controles na etapa de projeto da aplicação.

Uma aplicação pode ser dividida nos seguintes segmentos: Entrada (dado original e dado de entrada); Processamento de transação; Dado de saída (distribuição de resultados) e segurança (log, comunicações e armazenamento). Os controles em uma aplicação são implementados em cada segmento juntamente com restrições acesso à aplicação e a arquivos originais.

Embora não seja viável oferecer testes detalhados e checklists para cada possível entrada em uma aplicação, um auditor de TI deve conhecer os conceitos de controle que são comuns a quase todas as aplicações. Isso permite o surgimento de ideias de testes de auditoria mais específicos para a aplicação.

Alguns dos elementos de controle mais comuns são:

| | |
|---|---|
| Controles de Entrada | Entrada de dados/verificação de campos (Exemplo: |

| | |
|---|---|
| | Validação de número de cartão de crédito).<br>Gerenciamento de documentos originais (Exemplo: procedimentos de preparo e retenção).<br>Mecanismos de tratamento de Erros<br>Segregação de tarefas |
| Controles de Processamento | Mapeamento de regras de negócio.<br>Verificação de integridade e completude.<br>Cálculos automáticos.<br>Consolidação de entrada. |
| Controles de Saída | Validação de completude e precisão, consolidação.<br>Revisão e rastreabilidade de saída.<br>Revisão e monitoramento de relatórios de exceção.<br>Procedimentos de identificação de saída, tratamento, retenção e distribuição. |
| Controles de Segurança de Aplicação | Mecanismos de rastreabilidade (trilhas de auditoria, log, identificadores únicos).<br>Controle de acesso lógico a funcionalidades.<br>Proteção a dados armazenados. |

**Tabela 5 - Elementos de Controle mais comuns**

### 8.1.1 Controles de Entrada

Os objetivos dos controles de entrada é validar e autenticar ações de preparo e autorização de forma que dados precisos, confiáveis e completos sejam aceitos pela aplicação de forma adequada.

Uma proporção significativa dessas medidas é projetada na etapa de desenvolvimento de uma aplicação após o estabelecimento de regras de negócio. Enquanto dados de entrada podem ser manuais ou automatizados, erros e omissões podem ser minimizados por meio de projeto, segregação adequada de tarefas concernentes à origem e a aprovação de documentos de entrada, estabelecimento de autenticidade relevante, precisão e verificações de completude.

| Elementos de controle de entrada | Descrição |
|---|---|
| Verificações de dados de entrada | Verificações de validade automática em dados de entrada.<br>Verificações de completude para verificar que todas as informações de transações chave foram inseridas.<br>Verificações duplas comparando novas transações com transações anteriores. (Evitar duplicidade). |
| Gerenciamento de documentos de origem | Procedimentos de preparo de documentação<br>Log de documentos de origem<br>Numeração dos documentos (rastreabilidade)<br>Procedimentos de retenção de documentos. |

| | |
|---|---|
| Procedimentos de tratamento de erros | Procedimentos para lidar com dado de entrada rejeitado (Ex. mensagem de erro, medidas de correção subsequentes, reentrada de dados imediata, uso de dado suspenso). |
| Autorização de entrada | Procedimentos manuais em nível de supervisão para autorizar entrada de dados em formulário. Ex. Autorização de detalhes de entrada por um supervisor antes da entrada de dados por um operador. |

Tabela 6 - Elementos de controle de entrada

### 8.1.2 Controles de Processamento

O objetivo de medidas de controle de processamento é a proteção da integridade, validade e confiabilidade de dados e sua guarda contra erros de processamento ao longo do seu ciclo de vida, desde o momento da recepção no subsistema de entrada até seu envio ao banco de dados, transmissão ou saída em outro subsistema. Eles também asseguram que um dado de entrada válido é processado somente uma vez e que a detecção de transações erradas não interrompa o processamento das transações válidas. Ainda, buscam aumentar a confiabilidade da aplicação para atingir os requisitos do usuário.

Os procedimentos de controle incluem o estabelecimento e implementação de mecanismos que autorizem o início do processamento de uma transação e garantir que somente aplicações e ferramentas apropriadas e autorizadas estejam em uso. Eles verificam rotineiramente que o processamento é realizado de forma completa e precisa com os controles automatizados.

Os tipos de controle podem incluir verificação para erros de sequência ou duplicidade, contagem de transações/registros, verificação de integridade referencial, controles de totalizações, verificações de limites e sobrecargas de fila.

Em sistemas de tempo real alguns dos controles compensatórios podem ser de checagem individual e batching retrospectivo.

### 8.1.3 Controles de Saída

São medidas que asseguram que os dados de saída da aplicação sejam completos, precisos e corretamente distribuídos. Eles também visam proteger os dados processados de modificação e distribuição não autorizada.

Incluem definições de saídas apropriadas, relatórios e documentações de lógica de extração de relatórios, controles que limitem acesso a dados processados, revisão e consolidação de dados de saída.

### 8.1.4 Controles de Segurança de Aplicação

A segurança da aplicação se preocupa com a manutenção da confiabilidade, integridade e disponibilidade da informação na camada de aplicação. Para auditoria é importante compreender essas interfaces. Ex. diferentes origens de dados de entrada e saída e também como são armazenados.

A maioria das aplicações é acessada por meio de identificadores e senhas de usuário individuais. Entretanto, outras formas de login, como mecanismos Single Sign-on, têm se tornado populares dada a magnitude das aplicações utilizadas em um ambiente corporativo. Portanto, o controle de acesso do usuário deve ser entendido previamente. O auditor pode precisar revisar a política e procedimentos da entidade para obtenção e revogação de acesso ao usuário de forma a compreender a extensão a qual as regras estão implementadas e garantir que a aplicação tenha controles para concessão e remoção de acesso.

Para compreender os procedimentos de controle de segurança de aplicação, o auditor precisa entender os atores, papéis e responsabilidades envolvidas na aplicação, como administradores, usuários prioritários, usuários regulares etc.

O projeto do módulo de controle de acesso lógico pode se dar de várias maneiras. O acesso pode ser controlado em cada módulo, opção de menu, cada tela ou controlado por objetos e papéis. O Analista de Controle Externo deve rever o projeto do módulo de controle de acesso tendo em mente a criticidade das funções e ações disponíveis. Ainda, é necessária a capacidade de reconhecer mecanismos usados para garantia da autoria e

rastreabilidade das transações assim como a proteção aos dados armazenados.

Uma lista exemplificativa de questões a respeito de controles de segurança da aplicação:

- Rastreabilidade das transações: logs de transação, uso de identificador único de usuário, relatórios de log e monitoramento. O log de auditoria deve refletir os registros e campos alterados, quando foram alterados, quais alterações foram feitas e quem as fez.
- Gerenciamento de contas de usuário, permissões e senha: uso de contas de convidado, teste e genéricas, uso contas com acesso privilegiado e administradoras, controles compensatórios, procedimentos para atribuição e revogação de acesso, procedimentos de atribuição e remoção de permissão de acordo com a atividade, adoção do princípio do menor privilégio, acesso à equipe de TI a bases de produção, procedimentos formais para aprovação e atribuição de acesso, uso de senhas fortes, obrigatoriedade de mudanças periódicas, criptografia de senhas e etc.
- Proteção a arquivos e dados permanentes: Controles para garantir que alterações em dados permanentes sejam autorizadas, usuários sejam responsabilizados por cada mudança realizada, os dados permanentes sejam atualizados e exatos, a integridade dos arquivos seja mantida. Exemplos de dados permanentes: Detalhes de fornecedor e cliente (nome, endereço, telefone, conta bancária), taxas de inflação, dados de administração de sistema como senhas e permissões de controle de acesso, etc.

Tarefas conflitantes e adoção de segregação de tarefas: Diferentes papéis de usuário, disponibilidade de direitos de acesso para cada perfil e regras de segregação de funções.

## 8.2 RISCOS PARA A ENTIDADE AUDITADA

As consequências por falhas em controles de aplicação geralmente vão depender da sua natureza. Os riscos podem variar da insatisfação do usuário a desastres reais com perdas de vidas. Por exemplo, a confiança do cidadão nos serviços governamentais pode cair, a ausência de conformidade com a lei pode levar a processos, um serviço público essencial pode não chegar à casa das pessoas, finanças públicas podem ficar suscetíveis à fraude etc.

Mais precisamente, os riscos significativos possivelmente ocasionados pela ausência de controles de entrada apropriados, processamento errôneo ou fraudulento e pode levar a falhas a atingir objetivos do negócio. Os dados processados pela aplicação podem ser inconsistentes e saídas inapropriadas serão oferecidas pelos programas. Ainda, mesmo na presença de tais controles pode ser possível sobrepô-los em situações específicas. Nesse caso, devem haver controles compensatórios como logs e regras de autorização, de outro modo o privilégio sobreposto pode ser mal utilizado e levar a dados inconsistentes inseridos na aplicação.

Procedimento para gerenciamento de documentos de origem e autorização de entrada de dados são também um importante tipo de controle de entrada. Na ausência de gerenciamento apropriado de documentos, pode não ser possível rastrear a fonte da informação inserida no sistema, a conformidade com a lei pode não ser alcançada e as políticas de retenção podem ser infringidas, dados não confiáveis podem ser inseridos na aplicação, ainda, a ausência de controles de autorização pode levar a erros ou fraudes.

De modo geral, falhas em controles de processamento podem levar a erros e não atingimento dos objetivos de negócio da aplicação. Eles surgem do mapeamento incorreto das regras de negócio, teste inadequado de programas ou controle inadequado de diferentes versões. A ausência das práticas necessárias de controle de processamento pode ocasionar repetidas transações errôneas afetando os objetivos de negócio.

Em sistemas de processamento em tempo real, algumas medidas de controle como consolidação de dados totais de entrada e saída devem ser tomadas para averiguação de sua completude. Entretanto, sistemas de tempo real devem implementar outros controles compensatórios incluindo completude interativa de dados, avisos de validação, log de tentativas de acesso, etc.

A falta de controle de saída adequado leva a um risco de modificação/exclusão de dados não autorizada, criação de relatórios de gerenciamento mal customizados e até vazamento de dados.

No contexto de segurança da aplicação, a insuficiência de mecanismos de log pode tornar impossível a rastreabilidade da origem de falhas. Ainda, a consciência da necessidade de procedimentos de revisão de logs e mecanismos de relatórios pode mitigar o risco de mal uso de sistemas da informação. Erros em dados permanentes possuem efeito de longo alcance para a aplicação, já que esse dado pode ser usado por uma grande variedade de transações.

Na realidade, os riscos de não lidar apropriadamente com a segurança da informação podem ir muito além. Eles podem levar a consequências de variados graus de gravidade, incluindo: perda de receita, interrupção de serviços, perda de credibilidade, interrupção de negócio, mau uso da informação, consequências legais e abuso de propriedade intelectual.

# 9. TÓPICOS ADICIONAIS EM AUDITORIA DE TI

Esta seção oferece uma visão geral de alguns tópicos relacionados a Auditoria de TI que o analista pode se deparar ao longo de suas inspeções. Existem várias áreas que podem se tornar objetos auditáveis, então, o analista deve estar ciente destas e ser capaz de avalia-la adequadamente.

Ainda que essas áreas possam ter algumas diferenças ou aspectos específicos, elas podem ser auditadas utilizando as mesmas abordagens e técnicas que foram discutidas ao longo desse manual, mas possivelmente, demandando questões adicionais de auditoria.

## 9.1 WEBSITES/PORTAIS

Websites são sistemas da informação localizados na internet ou intranets que oferecem serviços e conteúdos como textos, imagens, vídeos, áudio e etc. Um portal organiza informações de diferentes fontes de uma maneira uniforme, oferecendo uma aparência e acesso uniformes. Normalmente, portais oferecem serviços como mecanismos de busca, notícias, informações, acesso a sistemas, bancos de dados e entretenimento (ISACA, 2012).

Um foco importante dentro da avaliação de Portais se dá na avaliação do cumprimento da legislação de Acesso à Informação por parte do cidadão, onde o analista deve avaliar a disponibilidade, integridade, autenticidade das informações bem como a existência de Política de Segurança entre outros aspectos presentes nas leis que regem o tema.

### 9.1.1 Áreas de Auditoria:

- Experiência do Usuário
- Segurança, Privacidade
- Tempo de Resposta
- Questões relacionadas à terceirização

## 9.2 COMPUTAÇÃO MÓVEL

Há um esforço crescente para o provimento de serviços ao público por meio de tecnologias de comunicação sem fio. Atualmente, muitas aplicações

estão disponíveis em ambiente móvel. Telefones celulares, tablets, redes wi-fi, TVs e uma ampla gama de novos serviços eletrônicos estão provendo informação.

A Computação Móvel pode ser vista como um ponto de acesso de TI (PC, laptop, etc.), mas eles tem algumas áreas de auditorias especiais que podem ser importantes.

### 9.2.1 Áreas de Auditoria

- Segurança sem fio, privacidade, criptografia.
- Experiência do usuário.
- Políticas específicas a respeito de computação móvel na organização.
- Riscos da utilização de dispositivos pessoais para acesso a dados e serviços corporativos.
- Riscos de acesso não autorizado a informação presente no dispositivo.
- Riscos crescentes de danos ou furtos de dispositivos corporativos.

## 9.3 AUDITORIA FORENSE (COMPUTAÇÃO FORENSE)

A Auditoria Forense é realizada para exame de mídias digitas para obtenção de evidências relacionadas a eventos específicos. A preservação de evidências é primordial durante uma análise forense. Ela inclui a abordagem, ferramentas e técnicas para examinar informações digitais para identificação, preservação, recuperação, análise e apresentação de fatos e opiniões sobre a informação armazenada.

É comumente associada a investigações criminais com vistas a oferecer evidências em um tribunal. A computação forense tem sido aplicada em inúmeras áreas incluindo, fraude, mal-uso de infraestrutura computacional, difamação, e-mails maliciosos, vazamento de informação, furto de propriedade intelectual, hackers e transferência ilegal de fundos.

### 9.3.1 Áreas de Auditoria

Envolve técnicas e princípios para recuperação de dados, mas com orientações e práticas destinadas a criação de uma trilha de auditoria.

- Retenção de evidências (dados, acesso, log) para análise.
- Captura e preservação de informação o mais perto do vazamento possível.
- Padrões de coleta de dados para possível uso legal.
- Processo de captura de dados minimamente invasivo sem interrupção das operações do negócio.
- Identificação de ataques quando possível.

## 9.4 GOVERNO ELETRÔNICO (E-GOV)

O advento da tecnologia da informação mudou como os governos oferecem serviços a seus cidadãos. Enquanto a tecnologia se dissemina por toda a população, os governos se preocupam com novas abordagens para a entrega de informação e aplicações para o benefício público. O Governo Eletrônico, governança eletrônica (conhecido como e-gov) e a governança móvel são algumas áreas que lidam a esse respeito. Esses conceitos estão relacionados embora não sejam exatamente sinônimos.

### 9.4.1 Áreas de Auditoria

Para o propósito da auditoria, o analista deve estar ciente de que a governança é normalmente exigida para oferecer serviços de maneira econômica, eficiente e efetiva. Em uma perspectiva de auditoria, a auditoria de sistemas da informação ou processos de negócio envolvidos em uma estratégia e-gov ou m-gov não se diferencia de uma auditoria tradicional de TI. O auditor deve observar algumas políticas adicionais e mecanismos de coerção (por exemplo, uma política organizacional em computação móvel, criptografia de software, limite a uso de smartphones, etc.).

## 10. CONCLUSÃO

O Papel da Auditoria de Tecnologia da Informação na garantia de que os processos apropriados estejam estabelecidos de modo a gerenciar os riscos e vulnerabilidades é crucial, principalmente levando em conta que os Tribunais de Contas têm como função precípua a avaliação da eficiência, efetividade e economicidade de toda a Administração Pública.

Já os Sistemas de Tecnologia da Informação devem assegurar a proteção da informação e bens públicos assim como apoiar a missão estratégica, as finanças públicas, entre outros objetivos.

Pensando nisso, a Organização Internacional de Entidades Fiscalizadoras Superiores (INTOSAI) desenvolveu um Grupo de Trabalho em Auditoria de TI (WGITA) que, ao longo dos anos, tem produzido material atualizado com vistas em fornecer aos Auditores de TI das SAI padrões e boas práticas universalmente reconhecidas.

Seguindo essas orientações, esperamos que o Manual de Auditoria de Tecnologia da Informação do Tribunal de Contas do Estado do Amazonas possa contribuir de forma abrangente com as principais áreas em que a Auditoria de TI se faz necessária, seguindo os princípios gerais de auditoria baseados em Padrões Internacionais para Instituições Superiores em Auditoria (ISSAI), bem como as práticas presentes em Frameworks Internacionais de TI reconhecidos, incluindo o Framework Cobit da ISACA, Padrões ISO (International Standards Organization), visando também oferecer aos Auditores de TI um conjunto completo de orientações sobre o tema.

Como objetivo principal, esse Manual fornece informações essenciais e perguntas-chave para um planejamento efetivo da Auditoria de TI. A expectativa é que ele seja útil para o Tribunal de Contas do Estado do Amazonas que, por meio da Diretoria de Controle Externo em Tecnologia da Informação (DIATI) tem atuado incessantemente na melhoria contínua dos controles relacionados a Bens e Serviços de TI ao longo dos anos.

## OBRAS CONSULTADAS


Auditor-General's Office Singapore. (2009). *What is an IT Audit.* Acesso em 07 de abril de 2017, disponível em Auditor-General's Office Singapore: http://www.ago.gov.sg/docs/default-source/brochure/197b4897-87d6-477d-9bc2-d06afa225a41.pdf

AXELOS. (20 de maio de 2017). *ITIL.* Acesso em 14 de maio de 2018, disponível em Axelos Global Best Practice: https://www.axelos.com/best-practice-solutions/itil

BERGAMI, P. R. (10 de outubro de 2013). *Qualidade de TI - Qual a Abrangência*. Acesso em 01 de fevereiro de 2018, disponível em TI Especialistas: http://www.publicadireito.com.br/artigos/?cod=7575c8affdb79557

BRAZ, M. (2017). *Auditoria de TI - O Guia de Sobrevivência.* Brasília.

DUTRA, E. C. (02 de 2017). *Auditoria de Sistemas de Informação.* Acesso em 01 de 02 de 2018, disponível em JUS.com.br: https://jus.com.br/artigos/56084/auditoria-de-sistemas-de-informacao-introducao-controles-organizacionais-e-operacionais

INTOSAI. (01 de outubro de 1977). *Declaração de Lima.* Acesso em 1 de junho de 2018, disponível em Biblioteca Digital TCU: http://portal.tcu.gov.br/biblioteca-digital/declaracao-de-lima.htm

INTOSAI. (12 de fevereiro de 2013). *IDI Handbook on IT Audit for Superme Audit Institutions.* Acesso em 03 de março de 2018, disponível em INTOSAI: http://icisa.cag.gov.in/resource_files/c60986ef8dd5d4f658df077c1b5dceb7.PDF

INTOSAI. (24 de maio de 2013). *ISSAI 100.* Acesso em 09 de 05 de 2018, disponível em Princípios Fundamentais de Auditoria de Setor Público: http://portal.tcu.gov.br/fiscalizacao-e-controle/auditoria/issai-em-portugues.htm

INTOSAI. (2014). *ISSAI 1315.* Acesso em 01 de 02 de 2018, disponível em Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and its Environment: http://www.issai.org/en_us/site-issai/issai-framework/4-auditing-guidelines.htm

INTOSAI. (2016). *ISSAI 5300.* Vienna: INTOSAI.

ISACA. (junho de 2012). *COBIT 5 - Modelo Corporativo para Governança e Gestão de TI.* Rolling Meadows - IL, EUA: ISACA.

ISACA. (janeiro de 2018). *COBIT 5 e o Valor Agregado da Governança da TI Corporativa.* Acesso em 20 de fevereiro de 2018, disponível em ISACA: http://www.isaca.org/COBIT/focus/Pages/cobit-5-and-the-added-value-of-governance-of-enterprise-it-portuguese.aspx

IT PEDIA. (17 de abril de 2017). *Which audit can we do?* Acesso em 17 de abril de 2018, disponível em IT PEDIA: https://www.itpedia.nl/en/2011/01/10/welke-audit-gaan-we-doen/

Ministério do Planejamento, Desenvolvimento e Gestão. (2017). *Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação.* Acesso em 01 de 02 de 2018, disponível em Governo Digital.gov: https://www.governodigital.gov.br/documentos-e-arquivos/Guia_de_Boas_Praticas_v3.pdf

NASCIMENTO, J. (janeiro de 2010). *Governança de TI e a ISO/IEC 38500.* Acesso em 01 de junho de 2018, disponível em Portal GSTI: https://www.portalgsti.com.br/2009/11/governanca-de-ti-e-isoiec-38500.html

NUNES, B. O. (06 de setembro de 2012). *COBIT – Características Gerais – Baseado em Controles*. Acesso em 12 de maio de 2018, disponível em Gestão de TI Inteligente: http://tiinteligente.blogspot.com/2012/09/cobit-caracteristicas-gerais-baseado-em.html

Portal de Auditoria. (02 de dezembro de 2016). *Testes de Auditoria.* Acesso em 15 de 03 de 2018, disponível em Portal de Auditoria: https://portaldeauditoria.com.br/testes-em-auditoria-uma-revisao-conceitual-aplicavel-na-pratica/

Portal de Auditoria. (fevereiro de 2018). *Controles Internos.* Acesso em 2 de abril de 2018, disponível em Portal de Auditoria: https://portaldeauditoria.com.br/controle-interno/

SEBRAE. (2017). *Planejamento Estratégico*. Acesso em 09 de maio de 2018, disponível em SEBRAE: http://bis.sebrae.com.br/bis/download.zhtml?t=D&uid=B6270FF790B50CB283257589005BE2D1

Secretaria dos Portos do Pará. (10 de 2016). *Comitê Gestor de Tecnologia da Informação - CGTI/CDP.* Acesso em 01 de 02 de 2018, disponível em Papel do CGTI: https://www.cdp.com.br/papel-do-cgti

Software Engineering Institute. (15 de novembro de 2010). *CMMI for Acquisition, Version 1.3.* Acesso em 02 de maio de 2018, disponível em SEI.edu: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2010_005_001_15284.pdf

Strong Security. (26 de julho de 2017). *Análise de Riscos em TI.* Acesso em 01 de abril de 2018, disponível em Strong Security : https://www.strongsecurity.com.br/analise-de-riscos-em-ti-o-que-e-como-fazer-e-mais/

TCE/AM. (16 de junho de 2002). *Regimento Interno.* Acesso em 03 de maio de 2018, disponível em Regimento Interno - Tribunal de Contas do Estado do Amazonas: http://www.insightgeopolitico.com/copa-do-mundo-e-geopolitica/

WETHERALL, J. D., & TANENBAUM, A. S. (05 de fevereiro de 2011). *Redes de Computadores.* Pearson.