TCEPR

TRIBUNAL DE CONTAS DO ESTADO DO PARANÁ

GUIA BÁSICO DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

NÚCLEO DE AUDITORIAS DE TI - NAUTI
COORDENADORIA DE FISCALIZAÇÕES ESPECÍFICAS - COFE

2017

SUMÁRIO

OS OBJETIVOS DESTE GUIA

A ideia deste guia nasceu do levantamento realizado pelo TCEPR em 2016 sobre o panorama do uso da Tecnologia da Informação (TI) na Administração Pública Municipal no Paraná. Os resultados, apresentados em relatório disponível na página internet do TCEPR, apontaram diversas carências na gestão de TI, com consequências potencialmente danosas aos municípios e seus cidadãos.

O objetivo principal deste guia é sensibilizar os gestores públicos, bem como os profissionais envolvidos com a área de TI na Administração Pública sobre aspectos fundamentais da Governança de TI, capazes de melhorar a qualidade dos gastos públicos, com acréscimo dos benefícios gerados pela TI para a população e diminuição dos riscos associados às operações de TI na Administração Pública.

Utilizando uma abordagem simples e lúdica, este guia trata do tema da Governança de TI de forma concisa e direta. É particularmente indicado aos profissionais que ainda não tem familiaridade com o tema da Governança de TI ou que o conhecem parcialmente.

Contudo, o profissional experiente em Governança de TI, por meio deste guia, poderá conferir os principais desafios encontrados na área de TI da Administração Pública Municipal e poderá utilizar este guia como suporte didático para sensibilizar profissionais da área de TI, assim como de outras áreas, sobre a importância da Governança de TI nas organizações.

O QUE É GOVERNANÇA DE TI?

"Governança de TI é uma estrutura de relacionamentos e processos para **dirigir** e **controlar** a TI a fim de **alcançar as metas da instituição** pela agregação de valor, enquanto se mantém o equilíbrio dos riscos versus retorno sobre esta função e seus processos. "

(ITGI – *IT Governance Institute*)

"Governança de TI é o sistema pelo qual o uso atual e futuro da TI é dirigido e controlado." (NBR ISO/IEC 38500, item 1.6.3)

FOCOS DA GOVERNANÇA DE TI:

- DIREÇÃO E CONTROLE
- ENTREGA DE VALOR

GOVERNANÇA DE TI E GESTÃO DE TI NA ADMINISTRAÇÃO PÚBLICA:

QUAIS SÃO AS DIFERENÇAS?

GOVERNANÇA DE TI

Estabelece REGRAS e MECANISMOS para dirigir e controlar a gestão da TI com o objetivo de atender aos interesses da Administração Pública e da sociedade.

A governança é sempre responsabilidade da alta administração de uma organização e não pode ser delegada para outras organizações (terceirizada).

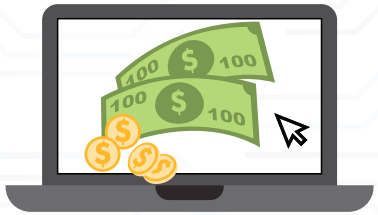
GESTÃO DE TI

PLANEJA, DESENVOLVE, EXECUTA E MONITORA as atividades de TI em consonância com as REGRAS e MECANISMOS estabelecidos a fim de atingir os objetivos da Administração Pública.

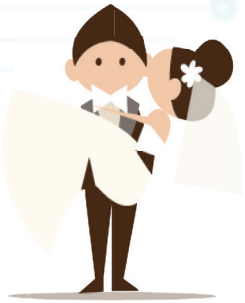
A gestão pode ser delegada para outras organizações (terceirizada), desde que haja uma governança adequada.

POR QUE A ADMINISTRAÇÃO PÚBLICA DEVE DAR IMPORTÂNCIA PARA A GOVERNANÇA DE TI?

1. **A TI é cara:** Os equipamentos e sistemas de TI consomem uma fatia importante do orçamento das organizações, além disso, ficam obsoletos rapidamente, exigindo constantemente novos investimentos.

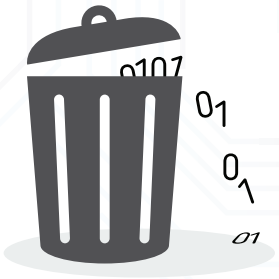


2. **É difícil voltar atrás nas decisões da TI:** As escolhas estratégicas de TI têm consequências duradouras que não podem ser mudadas facilmente. Estas decisões podem ser comparadas a casamentos, feitos para durar, mas que podem terminar em um divórcio litigioso, custoso e com aborrecimentos. Para realizar a troca de um sistema por outro, por exemplo, pode ser necessário cancelar contratos, treinar novamente todos os usuários e trocar computadores e bancos de dados.



3. **Panes na TI causam transtornos à Administração e à sociedade:** A TI está cada vez mais presente em várias áreas da Administração Pública, portanto interrupções em seus equipamentos e sistemas prejudicam ou mesmo impossibilitam o seu funcionamento.

4. **Dados perdidos podem ser irrecuperáveis:** Cada vez mais, os dados da Administração Pública são armazenados em computadores. A perda, a destruição ou o apagamento definitivo, intencional ou acidental, de informações que podem também conter registros de valores, ocasiona danos irreparáveis tanto aos cidadãos quanto ao Erário.



5. **A TI tem que trazer benefícios concretos:** A capacidade da TI de tornar os processos mais eficientes, econômicos, integrados e com melhor qualidade, deve ser intensificada ao máximo. Os investimentos realizados em TI devem resultar em melhorias percebíveis para a Administração Pública e para a sociedade.

COMO IDENTIFICAR QUANDO É NECESSÁRIO MELHORAR A GOVERNANÇA DE TI?

QUANDO...

- Não há responsável nem estrutura de TI formalmente estabelecidos no organograma.
- Fornecedores de serviços de TI desempenham funções reservadas à Administração Pública.
- A Administração não está preparada para assumir os sistemas ou substituir seus fornecedores.
- A Administração Pública não tem acesso direto às suas próprias bases de dados.
- A fiscalização dos contratos não garante que o que foi contratado foi entregue.
- Há perda de dados, invasões cibernéticas, acessos indevidos ou interrupções prolongadas dos sistemas.
- Não há ***backup*** periódico mantido em local seguro, distante dos dados originais e desconectado da rede.
- Não há ***firewalls*** nem antivírus que protejam os computadores contra invasões.
- Não há controle de acesso aos computadores.
- A sociedade não percebe os benefícios produzidos pela TI.

SITUAÇÕES QUE REQUEREM ATENÇÃO!

O TCEPR selecionou algumas situações de risco relacionadas à TI que representam perigo potencial para a administração pública e procurou relacionar os pontos que permitam aos gestores públicos e profissionais de TI identificar facilmente indícios destas ocorrências. As situações de risco descritas nas próximas páginas são causadas por planejamento inadequado, falha no controle, desalinhamento da TI com as estratégias da organização e descuido com segurança.

APRISIONAMENTO TECNOLÓGICO

Ocorre quando há dificuldade ou impossibilidade de trocar de fornecedor ou manter os sistemas funcionando após o fim do contrato. As seguintes situações podem levar a aprisionamento tecnológico:

- Bases de dados localizadas apenas em local externo. (Ex.: nas dependências dos fornecedores)
- Impossibilidade de acessar diretamente as próprias bases de dados.
- A funcionalidade de exportar as bases de dados não está disponível.
- A funcionalidade de auditar os sistemas não está disponível.
- Impossibilidade de acessar o código-fonte atualizado, se houve aquisição da propriedade intelectual dos sistemas.
- Ausência de documentação atualizada sobre as regras de negócio dos sistemas.
- Ausência de modelos atualizados dos bancos de dados dos sistemas.
- Dependência do fornecedor para manter os sistemas funcionando.
- Os fornecedores executam funções exclusivas da Administração Pública.

FALHA NO CONTROLE

FALHA NA CONTRATAÇÃO

PROJETO BÁSICO OU TERMO DE REFERÊNCIA DEFICIENTES

Quando estes documentos estão incompletos ou incorretos, a contratação de fornecedores de soluções de TI pode apresentar desde o início problemas difíceis de serem solucionados. As seguintes situações podem indicar que o Projeto Básico ou o Termo de Referência são deficientes:

- Detalhamento insuficiente do objeto (descrição genérica do que se quer contratar).
- Inexistência de justificativa para os quantitativos demandados.
- Desalinhamento com as estratégias da organização.
- Ausência de justificativas para a contratação, que supram necessidades da Administração e da sociedade.
- Quebra do princípio da isonomia, com restrições à livre concorrência (direcionamento).
- Ausência de ANS (Acordo de Nível de Serviço), que estipule tempos de resposta para as solicitações.
- Ausência de sanções para o descumprimento do Acordo de Nível de Serviço.
- Ausência de procedimentos informatizados para o registro de solicitações de serviço.
- Ausência de Relatórios de Acompanhamento das solicitações de serviço.
- Contratação com pagamento por horas-homem.

SOLUÇÕES DE TI INADEQUADAS

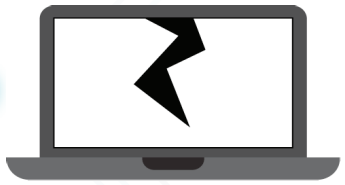
Soluções de TI que não atendem às reais necessidades da Administração resultam em mal-uso dos recursos públicos e por vezes são consequência de decisões estratégicas de TI que não envolvem todas as partes interessadas. As seguintes situações indicam que as soluções de TI são inadequadas:

- Apesar da utilização de sistemas, ainda se recorre ao uso de planilhas eletrônicas ou em papel.
- As soluções de TI não atendem a muitos cidadãos, mas apenas a uma pequena parte deles.
- A TI não promove simplificação, rapidez, aumento da segurança e da qualidade dos processos da Administração.
- A sociedade não percebe os benefícios das soluções de TI.
- Há diversas soluções de TI que não se integram adequadamente.
- Há trocas constantes de sistemas em decorrência da mudança de gestão (devido a decisões de caráter predominantemente político e pouco técnico).
- Há funções subutilizadas ou não utilizadas nos sistemas, apesar de adquiridas.

GESTÃO INAPROPRIADA DOS RISCOS

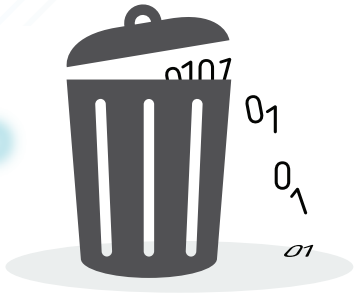
A área de TI comporta muitos riscos, tais como furtos e avarias em equipamentos, falhas em sistemas, acessos por pessoas não autorizadas, alteração ou eliminação indevida de dados, ataques cibernéticos, entre outros. A adoção de gestão de riscos, que os identifique e procure mitigá-los ou mesmo eliminá-los é indispensável para evitar as consequências desastrosas que podem derivar de incidentes na área de TI. As seguintes situações podem indicar que a Gestão de Riscos de TI é inadequada:

1. **Interrupções em equipamentos:** Todo equipamento tem vida útil finita e em algum momento irá falhar. Manter equipamentos de reserva ou prever no contrato de compra ou locação o fornecimento tempestivo de equipamentos substitutivos, em caso de falhas, pode encurtar o tempo de indisponibilidade dos equipamentos e consequentemente dos sistemas e processos que deles dependem, contribuindo para diminuir ou mesmo eliminar os danos e transtornos à Administração Pública causados pelas falhas.



2. **Interrupções em sistemas:** Programas de computador sempre estão sujeitos a falhas porque não são produtos acabados e imutáveis. Com frequência são modificados para incorporar novas tecnologias e funcionalidades. É imprescindível contar com suporte para que falhas nos sistemas sejam sanadas tempestivamente, diminuindo o tempo de indisponibilidade. No caso de contratação de suporte terceirizado, deve-se considerar a modalidade de atendimento remoto, via telefone ou internet, que contribui para a solução rápida dos problemas em localidades que não contam com atendimento presencial.

3. **Perda de dados:** A ausência de processos de backup (cópia de segurança) confiáveis pode acarretar na perda irreversível de dados. Para se precaver contra a perda acidental ou intencional de dados, é necessário que os backups ocorram com frequência ao menos diária e que seja mantida uma cópia atualizada do backup em local seguro, distante dos servidores que armazenam os dados originais e desconectado da rede, para impedir invasões cibernéticas pela internet. Além disso, é necessário realizar periodicamente testes de recuperação dos dados armazenados, de modo a verificar que sejam realmente recuperáveis.



4. **Sistemas não auditáveis:** Quando os sistemas não são auditáveis, não é possível rastrear alterações no código e nas bases de dados dos sistemas. Todos os sistemas da Administração Pública devem ser auditáveis para que seja possível rastrear as operações de consulta, inclusão, exclusão e alteração de dados. Os registros das operações devem armazenar detalhes das operações, incluindo o tipo de operação realizada, data, horário e usuário que a realizou. Sistemas não auditáveis são alvos preferenciais para fraudes, pois costumam não deixar registros que permitiriam identificar o ilícito e seus responsáveis.

5. **Acessos indevidos:** Sistemas com controle de acesso falho ou inexistente facilitam a utilização por pessoas não autorizadas, para consultar, alterar ou mesmo eliminar dados indevidamente, de modo intencional ou acidental, com graves consequências para a Administração Pública, que pode ter seus dados sigilosos revelados e registros de créditos alterados ou cancelados. O estabelecimento de uma política de controle de acesso aos sistemas, incluindo regras para definição e trocas de senhas, é essencial para se precaver contra os problemas decorrentes de acessos indevidos.

6. **Invasões cibernéticas:** As invasões cibernéticas representam um risco real para a Administração, com potencial perda de controle sobre os seus sistemas e dados. Entre os ilícitos cometidos pelos invasores, é particularmente danosa a prática de criptografar as bases de dados e sistemas, de modo a torná-los inacessíveis para a Administração. Trata-se de prática criminosa de difícil combate, pois geralmente provém de países distantes do alcance da justiça brasileira. É possível precaver-se contra as invasões por meio da implementação de barreiras de proteção (firewalls) à rede da Administração e mantendo backups diários dos sistemas e dados da Administração Pública, em local seguro e desconectado da rede, para permitir a sua recuperação em caso de invasões.

IMPLANTAR A GOVERNANÇA DE TI: ROTEIRO EM 3 ETAPAS

Com o objetivo de orientar para uma melhoria gradual da Governança de TI na Administração, o TCEPR reuniu alguns mecanismos e instrumentos, agrupando-os em 3 etapas, partindo das iniciativas mais simples para as mais complexas.

A primeira etapa contém iniciativas de rápida implementação e a baixo custo, capazes de produzir resultados imediatos utilizando recursos existentes. Tem o seu foco na produção de documentos, na definição de políticas e na formalização de estruturas organizacionais.

Na segunda etapa, o foco está na contratação de soluções de TI, no seu planejamento e controle. Alguns dos resultados esperados podem ser percebíveis somente nas contratações futuras.

A terceira etapa é a mais complexa e a que exige maior preparação. Inclui a implantação de melhores práticas e normas nacionais e internacionais reconhecidas como eficazes na melhoria da governança de TI e que produzem resultados duradouros.

ETAPA 1

1. Designação formal do responsável pela TI
2. Organograma da área de TI
3. Descrição dos cargos e funções de TI
4. Política de Segurança da Informação
5. Comitê de TI
6. Catálogo de serviços de TI
7. Gestão e Fiscalização de Contratos
8. PCN (Plano de Continuidade dos Negócios) ou Plano de Contingência
9. Índices (e metas) de desempenho para a TI
10. Promoção da transparência

1. Designação formal do responsável pela TI: O profissional formalmente designado é legitimado para representar e defender os interesses da área de TI e a participar das decisões estratégicas juntamente com coordenadores de outras áreas, o que contribui para o alinhamento da TI com os objetivos da organização. A designação favorece a dedicação exclusiva do responsável e reforça sua autoridade e capacidade de comando para que a TI atinja os seus objetivos.

2. Organograma da área de TI: Estrutura hierárquica formal da área de TI, representando simultaneamente os diferentes elementos do grupo funcional e as suas ligações e responsabilidades. Ao distinguir e formalizar os diversos cargos da área de TI e suas relações com pares, superiores e subordinados, o organograma de TI reforça a segregação de funções, contribui para a valorização e responsabilização dos seus profissionais e promove a transparência da área de TI.

3. Descrição dos cargos e funções de TI: Documento que descreve as atividades, responsabilidades e requisitos técnicos e comportamentais para os cargos da área da TI. Possibilita que os profissionais de TI conheçam precisamente suas atribuições, reponsabilidades e metas. Permite a distribuição mais eficiente de tarefas entre os profissionais de TI e facilita o planejamento de treinamentos para cobrir possíveis lacunas no conhecimento e nas habilidades de seus profissionais.

4. Política de Segurança da Informação: Documento que contém orientações e regras para a proteção das informações em uma organização. Visa preservar a **confidencialidade**, a **integridade** e a **disponibilidade** das informações e se sustenta em 3 pilares: **pessoas, processos e tecnologia.** Aborda as seguintes questões:

- Responsabilidade das diversas categorias de profissionais na guarda, manuseio e disponibilização das informações.
- Estabelecimento e funcionamento do comitê de segurança da informação.
- Regras para o correto uso do correio eletrônico e da internet.
- Controle de acesso aos sistemas via autenticação e senha.
- Uso dos computadores, periféricos e dispositivos móveis.
- Acesso controlado ao Datacenter.
- Política de backups (cópias de segurança).
- Medidas de proteção contra ameaças cibernéticas (manter os sistemas operacionais, antivírus e *firewalls* atualizados).
- Planejamento e realização de auditorias dos sistemas e dados.

5. Comitê de TI: Tem a função de discutir, priorizar e decidir sobre as questões estratégicas de TI, alinhado com as estratégias da organização. Para que seja efetivo, deve ser constituído formalmente, se reunir periodicamente e ser composto por membros representantes de diversas áreas ou partes interessadas, incluindo necessariamente a direção da organização e profissionais da área de TI.

6. Catálogo de serviços de TI: Lista descritiva dos serviços ofertados pela TI. No contexto da Administração Pública, o catálogo é destinado a usuários internos (funcionários) e externos (sociedade). São exemplos de serviços aos usuários internos: instalação de computadores, treinamento sobre os sistemas etc. E aos externos: Emissão de guias, certidões e extratos por meio de portais na internet.

7. Gestão e Fiscalização dos Contratos: Para assegurar que os objetos do contrato (produtos e serviços de TI) sejam entregues com a qualidade, prazo e custos acordados, é necessário que gestores e fiscais de contrato comparem as entregas dos fornecedores com o estabelecido nos contratos, aplicando as sanções previstas ou a rescisão, nos casos de inconformidades. Para todo contrato deve haver um histórico de todos os registros importantes durante sua vigência. O exercício da função de gestor e fiscal de contrato exige preparação, empenho e implica em grandes responsabilidades, portanto é imprescindível que estes profissionais recebam treinamento apropriado e disponham de tempo suficiente para gerir e fiscalizar os contratos sob sua responsabilidade.

8. PCN (Plano de Continuidade dos Negócios) ou Plano de Contingência: Na área de TI, o PCN é um conjunto de procedimentos para o reestabelecimento das operações de TI após desastres (incêndio, enchente, furto de computadores, ataques cibernéticos, avarias em equipamentos, entre outros). O PCN deve estar sempre atualizado, impresso e disponível em local de fácil acesso aos responsáveis pela recuperação. Deve conter todas as instruções necessárias, passo-a-passo, para voltar a operar e normalizar o funcionamento dos sistemas o mais rapidamente possível. Além disso, para amenizar ou evitar os efeitos causados por interrupções inesperadas, são cabíveis as seguintes medidas:

- Contratação de serviços de substituição (temporária ou definitiva) de equipamentos como precaução contra avarias, falhas ou furtos.
- Contratação de suporte aos sistemas como precaução contra falhas que impliquem em mau funcionamento ou interrupção das operações.
- Contratação de suporte remoto aos sistemas para as localidades onde seja dificultoso providenciar o deslocamento de um profissional de suporte.
- Utilização de nobreaks ou geradores contra interrupções de energia que possam afetar serviços essenciais (sistemas hospitalares, de trânsito, etc.).
- Implantação e manutenção de procedimentos seguros e periódicos de backup (cópias de segurança) dos sistemas e seus dados.

9. Indicadores (e metas) de desempenho para a TI: Os indicadores são um meio importante para mensurar o desempenho de processos, para apurar falhas e para verificar o cumprimento de metas. Na área de TI, podem ser utilizados indicadores para mensurar a eficiência e a eficácia dos processos, assim como para verificar o cumprimento de metas estabelecidas em contratos com fornecedores. Os indicadores devem ser atualizados e publicados periodicamente. São exemplos de indicadores de TI:

- Número de solicitações de ordens de serviço atendidas em determinado período.
- Tempo médio de atendimento das solicitações.
- Percentual de indisponibilidade dos sistemas.
- Nível de satisfação dos usuários (percentual de solicitações atendidas plenamente).
- Percentual de projetos concluídos dentro do prazo e orçamento previstos.

10. Promoção da transparência: A TI é uma importante ferramenta para promover a transparência na Administração Pública, permitindo a disponibilização de informações à sociedade de modo rápido, prático e a custos reduzidos. Muitas das informações armazenadas em bases de dados ou em arquivos de computadores podem ou mesmo devem ser disponibilizadas no portal da Administração Pública, para serem utilizadas pelos cidadãos e por observatórios que atuam no controle social. É essencial que sejam mantidas atualizadas e disponíveis na internet as seguintes informações:

- Estrutura organizacional da Administração Pública.
- Endereços e telefones das unidades da Administração, com horários de atendimento ao público.
- Registros de quaisquer repasses ou transferências de recursos financeiros.
- Informações sobre licitações, inclusive os editais e resultados.
- Dados gerais para o acompanhamento de programas, ações, projetos e obras do governo.
- Respostas a perguntas mais frequentes da sociedade.

ETAPA 2

1. Planejamento da Contratação
2. Comparação de preços
3. Soluções Gratuitas ou a Curto Reduzido
4. ANS (Acordo de Nível de Serviço)
5. Contratação com pagamento por resultados
6. Preparação para o fim do contrato

1. Planejamento da Contratação: As contratações de TI devem ser sempre precedidas de planejamento para evitar a aquisição de soluções inadequadas, que não atendam às necessidades da Administração e da sociedade. O planejamento da contratação deve incluir estudos de viabilidade técnica e financeira e justificativas suficientemente embasadas sobre a necessidade da contratação. O resultado do planejamento deve ser claro o bastante para que os licitantes e a sociedade em geral compreendam o que deve ser entregue pelos contratados, em que tempo e a qual custo.

2. Comparação de preços: Pode haver diferenças significativas de preços de produtos e serviços de TI entre diferentes fornecedores. Durante o processo de planejamento da contratação, deve-se realizar pesquisa de preços de mercado, utilizando contratos públicos de soluções similares, cotações de fornecedores, preços divulgados na internet e preços divulgados pelo site governamental "comprasnet" (http://www.comprasgovernamentais.gov.br/).

3. Soluções Gratuitas ou a Custo Reduzido: No âmbito da Administração Pública existem catálogos de softwares públicos que podem ser utilizados sem custo, para gestão acadêmica, controle de frota, tramitação de processos e gerenciamento de serviços de TI, entre outros. O uso de software público, ou ainda, de software livre ou produzido por outros órgãos da Administração Pública deve ser considerado antes de se optar pela aquisição ou licenciamento oneroso de software proprietário. Uma opção a custo reduzido pode ser a adesão a consórcios com outras organizações públicas, para dividir os custos de utilização de sistemas proprietários complexos, tais como sistemas contábeis e de recursos humanos, por exemplo.

4. Acordo de Nível de Serviço (ANS): Para que as soluções de TI produzam os resultados esperados, é importante estabelecer em contrato Acordos de Nível de Serviço que definam critérios de aceitação e qualidade para os serviços e produtos entregues. O cumprimento dos acordos deve ser monitorado por meio de relatórios que apresentem os registros das entregas efetuadas, com indicadores que permitam verificar a conformidade com os parâmetros estabelecidos. São exemplos de parâmetros para Acordos de Nível de Serviço: tempo para atendimento de solicitações, percentual de tempo de disponibilidade da internet, percentual de soluções entregues que foram aceitas pelos requisitantes. Para que o ANS seja efetivo, devem ser previstas e aplicadas sanções em caso de descumprimento do acordado.

5. Contratação com Pagamento por Resultados: A contratação tem por objetivo suprir uma necessidade concreta da Administração Pública, com entrega de serviços ou produtos que podem ser mensurados. O pagamento mediante confirmação de que a entrega corresponde ao contratado, contribui para a melhoria da eficiência do fornecedor e para a redução de custos. Em oposição, a contratação por horas-homem deve ser evitada, pois é desvantajosa para a Administração ao permitir a remuneração de horas improdutivas e a ocorrência do paradoxo lucro-incompetência, caracterizado pela situação em o fornecedor é beneficiado quando ineficiente, pois quanto mais horas emprega para entregar o contratado, maior é o seu lucro.

6. Preparação para o fim do contrato: Ao aproximar-se do fim dos contratos de fornecimento de soluções de TI, a Administração Pública deve preparar-se para assegurar que eventuais trocas de fornecedores ou sistemas não prejudiquem as operações e tampouco impliquem em perda de acesso às suas bases de dados. As seguintes ações podem auxiliar na preparação para o fim dos contratos de TI:

- Assegurar o acesso às bases de dados, às regras de negócio, à modelagem dos dados e aos vários manuais (de usuário, de instalação e configuração etc.), sempre atualizados.

- Assegurar o acesso aos códigos-fontes atualizados, quando se detém a propriedade intelectual dos sistemas.

- Preparar-se para realizar a transferência de tecnologia das operações, manutenção e evolução dos sistemas para a Administração Pública ou para outro fornecedor.

- Certificar-se que a Administração Pública possui a infraestrutura e os profissionais necessários para dar continuidade às operações, à manutenção e à evolução das soluções de TI, caso deseje assumir (internalizar) estas atividades.

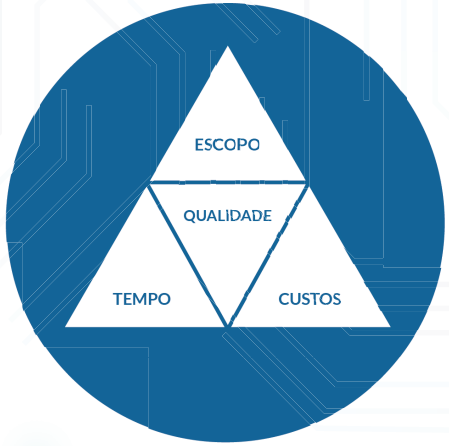
- Não realizar a aquisição onerosa dos códigos-fontes dos sistemas nos casos em que a Administração Pública não reúna as condições para assumir a continuidade da manutenção e desenvolvimento dos sistemas.

- Revisar o termo de referência das licitações planejadas e o contrato para certificar-se que incluam Acordos de Níveis de Serviço (ANS), alinhamento com o PETI ou PDTI, planilhas de cálculo dos quantitativos com valores unitários dos produtos e serviços.

ETAPA 3

1. Gerenciamento de Projetos
2. Gestão de Riscos
3. PETI (Plano Estratégico de TI)
4. PDTI (Plano Diretor de TI)
5. ITIL
6. COBIT

1. Gerenciamento de Projetos: Na área de TI, muitas das entregas são resultados de projetos que se diferenciam das operações por terem um início, meio e fim bem definidos e exigirem planejamento e controle do custo, tempo, prazo e qualidade. São exemplos de projetos de TI: implantação de infraestrutura de rede, desenvolvimento de sistemas, elaboração de PDTI, migração de dados de um sistema a outro. Para gerenciar projetos há diversas metodologias, algumas das quais largamente utilizadas na área de TI, como as metodologias ágeis (ex. SCRUM) para desenvolvimento de sistemas.



2. Gestão de Riscos: Na área de TI, são vários os eventos indesejados que podem causar transtornos à Administração Pública, com consequências danosas aos cidadãos e ao Erário. Muitos destes eventos são mitigáveis, ou mesmo eliminâveis, quando identificados antecipadamente em uma fase de planejamento de precaução contra riscos potenciais. É necessário levar em consideração que a relação custo-benefício da gestão de riscos deve ser aceitável, ou seja, a gestão de um risco não pode ser mais onerosa que as consequências de sua ocorrência. A gestão de riscos é composta pelas seguintes fases:

- Contextualização dos cenários de risco: Situações que podem ocorrer e probabilidade de ocorrência (ex.: há risco de inundação?).
- Identificação dos riscos: Se as situações identificadas ocorrerem, o que será afetado na TI da Administração Pública.
- Análise de riscos: Análise das consequências que a ocorrência identificada traria para a Administração Pública.
- Resposta aos riscos: Definir as ações para evitar ou mitigar o risco. Pode-se também transferir o risco para um terceiro (ex.: seguradora) ou mesmo aceitar o risco e preparar-se para a sua ocorrência.
- Monitorar e controlar os riscos: Realizar acompanhamento dos potenciais riscos, mantendo atualizado o documento de gestão de riscos, incluindo novos riscos, se necessário.

3. PETI (Plano Estratégico de TI): Documento que descreve as estratégias da TI para um determinado período. Tem por objetivo assegurar que as metas e objetivos de TI estejam alinhados com as estratégias da organização. No contexto da Administração Pública, o PETI deve delinear quais estratégias deverão ser adotadas pela TI de modo a atender as necessidades e anseios da Administração e da sociedade. O PETI deve ser revisado periodicamente e sempre validado pelo Comitê de TI.

4. PDTI (Plano Diretor de TI): Alinhado com o PETI, o PDTI descreve de que modo a TI atenderá as estratégias definidas para a TI na organização. Faz um diagnóstico da TI e estabelece metas a serem alcançadas e ações e projetos a serem desenvolvidos. As contratações de soluções de TI devem ser planejadas em harmonia com o estabelecido no PDTI.

5. ITIL: É um conjunto de boas práticas com foco nas áreas de operação e gerenciamento de serviços de TI. É particularmente útil e muito utilizado nos processos de service desk para o atendimento de solicitações de usuários da TI e tratamento de incidentes de TI. A adoção de ferramentas de service desk aderentes ao ITIL, também disponíveis comercialmente, contribui para a melhoria da governança de TI, pois possibilitam, entre outros benefícios, o registro e acompanhamento do andamento das solicitações, com a verificação da satisfação do usuário ao final do processo. O ITIL também auxilia na identificação de problemas recorrentes de TI e na busca de suas soluções.

6. COBIT: Conjunto de boas práticas para a governança e gestão de TI. É particularmente eficaz para traduzir as estratégias de uma organização em estratégias de TI e subsequentemente em ações práticas que permitam elevar a maturidade da governança de TI. A utilização do COBIT certamente pode contribuir para aumentar a capacidade da TI para entregar valor, gerenciar seus riscos e recursos, mensurar o seu desempenho e promover o alinhamento da TI com as estratégias da organização. O COBIT também pode ser usado como ferramenta para obter um diagnóstico e para traçar metas e objetivos para a TI.

ONDE ENCONTRAR MAIS INFORMAÇÕES SOBRE GOVERNANÇA DE TI?

Normas e Frameworks

- ISO/IEC 38500 - Governança Corporativa de Tecnologia da Informação
- ISO/IEC 27001 - Gestão de Segurança da Informação
- COBIT 4.1 e COBIT 5 - Control Objectives for Information and Related Technology
- ITIL - Information Technology Infrastructure Library

Guias de contratação de soluções de TI

- MPOG – SLTI – Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação – versão 2.0 (2014). Disponível em: http://cpsustentaveis.planejamento.gov.br/assets/conteudo/uploads/guia-de-boas-praticas-em-contratacao-de-solucoes-de-ti.pdf
- MPOG – SLTI - INSTRUÇÃO NORMATIVA Nº 4, DE 11 DE SETEMBRO DE 2014. Disponível em: http://www.governoeletronico.gov.br/documentos-e-arquivos/1%20-%20IN%204%20%2011-9-14.pdf

- MPOG – SLTI - Guia de Elaboração de PDTI Do SISP – Versão 1.0 (2012). Disponível em: http://sisp.gov.br/guiapdti/wiki/download/file/Guia_de_Elabora%C3%A7%C3%A3o_de_PDTI_v1.0_-_versao_digital_com_capa.pdf

- TCU – Guia de boas práticas em contratação de soluções de tecnologia da informação – versão 1.0 (2012). Disponível em: http://portal2.tcu.gov.br/portal/pls/portal/docs/2511467.PDF

- UFPR - Modelo de Contratação de Solução de Tecnologia da Informação Manual da etapa de Planejamento da Contratação, com base na IN MPOG/SLTI nº 04, de 11 de setembro de 2014. Disponível em: https://cce.ufpr.br/portal/wp-content/uploads/2015/05/Modelo_Contratacao_Solucao_TI.pdf

Notas Técnicas TCU

- Nota técnica Sefti 1 - conteúdo mínimo de termo de referência de TI. Disponível em: http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24F0A728E014F0B1F55B532FF&inline=1

- Nota técnica Sefti 2 - Uso do Pregão para Aquisição de Bens e Serviços de TI. Disponível em: http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24F0A728E014F0ADF50232727

- Nota técnica Sefti 6 - Aplicabilidade da Gestão de Nível de Serviço. Disponível em: http://www.tirio.org.br/admin/arquivo/arquivos/Nota-Tecnica-06-2010-Pagamento.pdf

Legislação de Apoio

- Lei Federal nº 8.666/1993 (Licitações e Contratos)
- Acórdãos TCU
- Constituição Estadual do Paraná
- Constituição Federal de 1988
- Instruções Normativas (SLTI/MPOG)
- Lei Complementar Estadual nº 113/2005 (Lei Orgânica do TCE-PR)
- Lei Complementar Federal nº 101/2000 (LRF)
- Lei Federal nº 13.019/2014 (Organizações Sociais)
- Lei Federal nº 8.429/1999 (Lei da Improbidade Administrativa)

GLOSSÁRIO

Antivírus: Programa que detecta e elimina vírus de computadores (certos programas danosos) e também impede sua instalação e propagação a outros computadores.

Backup: Cópia de segurança de dados e programas, mantida em dispositivos de armazenamento.

Código-fonte: Conjunto de instruções em linguagem de programação, na forma de palavras e símbolos ordenadas de maneira lógica e legível, que formam um programa de computador.

Erário: Conjunto dos bens e recursos financeiros públicos, que pertencem ao Estado.

Firewall: Barreira (solução de segurança) que tem o propósito de proteger uma rede interna de computadores contra comunicações indevidas com uma rede externa.

SCRUM: Metodologia ágil para o planejamento e gerenciamento de projetos de desenvolvimento de sistemas.

Service Desk: Atendimento ao usuário, com registro, análise e acompanhamento da solicitação até a obtenção do retorno do usuário sobre a eficácia da solução aplicada.

A cartilha está disponível on-line no endereço: http://www1.tce.pr.gov.br/multimidia/2017/5/pdf/00316351.pdf

TCEPR

Praça Nossa Senhora de Salette s/n | Centro Cívico | Curitiba | PR | CEP 80530-910