ORIENTAÇÕES TÉCNICAS

GERAIS DE TIC

VOL.3

[OT 011-015]

CGTIC

CIDADE DE SÃO PAULO
INOVAÇÃO E TECNOLOGIA

ORIENTAÇÕES TÉCNICAS

GERAIS DE TIC

VOL.3

[OT 011-015]

CGTIC

CIDADE DE SÃO PAULO
INOVAÇÃO E TECNOLOGIA

Coordenadoria de Gestão de Tecnologia da Informação e Comunicação
E-mail: http://tecnologia.prefeitura.sp.gov.br
Endereço: Rua Líbero Badaró, 425 — 4º andar — Centro
Telefone: 55 11 2392-2092

SUMÁRIO

APRESENTAÇÃO

As Orientações Técnicas são instrumentos de governança previstos pelo Decreto Municipal 57.653, de 07 de abril de 2017, o qual define a Política Municipal de Tecnologia da Informação e Comunicação. Estas visam auxiliar os órgãos do Sistema Municipal de Tecnologia da Informação e Comunicação (SMTIC) na implantação de soluções de tecnologia da informação e comunicação a fim de facilitar a convergência e o estabelecimento de padrões técnicos na Administração Pública Municipal, bem como consolidar práticas e ações aderentes à Politica Municipal de Governança de Tecnologia da Informação e Comunicação (PMGTIC).

Fazem parte de cada orientação técnica conteúdo normativo enunciado como recomendações, que estabelece padrões técnicos a serem seguidos, e também conteúdo de caráter não vinculante enunciado como sugestões, que visa orientar e estimular boas práticas e soluções em Tecnologia da Informação e Comunicação.

INTRODUÇÃO

O presente documento estabelece diversas diretrizes técnicas, gerais e específicas, para os Órgãos Setoriais da Prefeitura do Município de São Paulo. É parte integrante das Orientações Técnicas (OT) que foram estabelecidas como instrumento de Governança de Tecnologia da Informação e Comunicação – TIC no Decreto Municipal 57.653, de 07 de abril de 2017, que define a Política Municipal de Tecnologia da Informação e Comunicação.

O objetivo desta OT é padronizar procedimentos e processos de tomada de decisão, bem como disseminar conhecimentos e estimular boas práticas para que os Órgãos Setoriais possam conduzir suas iniciativas de forma embasada e de acordo com o seu grau de maturidade.

Fazem parte do escopo desse documento as diretrizes no que tange à padronização, boas práticas de uso, operação e segurança para a conexão física e lógica, com o objetivo de possibilitar o tráfego controlado de dados entre as redes envolvidas em um nível adequado de riscos.

Sendo a Tecnologia da Informação e Comunicação temática dinâmica e de soluções em constante evolução e transformação, essa Orientação Técnica poderá ser objeto de revisões posteriores, visando estar atualizada de acordo com os conhecimentos mais atuais e alinhada ao contexto da Prefeitura Municipal de São Paulo.

DEFINIÇÕES IMPORTANTES

Uma **recomendação** é uma diretriz definida pelo Conselho Municipal de Tecnologia da Informação e Comunicação – CMTIC, e estabelece regras, procedimentos ou critérios a serem seguidos por padrão. Desta forma, a sua não adoção deverá ser justificada tecnicamente.

Uma **sugestão** é uma boa prática validada pelo CMTIC e possui um caráter não vinculante, mostrando alternativas ou conhecimentos que poderão ser úteis na busca de soluções.

Os procedimentos descritos nestas Orientações Técnicas (OT-011/OT-015) deverão ser aplicados nos procedimentos atuais e futuros, bem como nos contratos e acordos futuros e nas prorrogações contratuais, ainda que de contratos assinados antes do início da vigência desta OT.

[OT 011]
DIRETRIZES PARA CONTRATOS DE SUSTENTAÇÃO DE TIC E SIMILARES

Visa orientar os servidores sobre contratações que envolvam desenvolvimento de sistemas, avaliar a possibilidade de separar, em contratos específicos, o desenvolvimento de sistemas de maior complexidade e/ou de maior importância estratégica.

EXECUÇÃO INDIRETA DOS SERVIÇOS DE TI

A Tecnologia da Informação (TI) tem se tornado, cada vez mais, elemento indispensável ao alcance dos objetivos organizacionais. No âmbito governamental, a legislação prioriza a execução indireta de tarefas executivas por meio da contratação de empresas para a prestação de serviços, de modo a ganhar especial relevância as contratações de serviços de TI efetuadas pelos órgãos e entidades.

Estas contratações, por sua vez, materializam-se por meio de contratos, que geralmente são decorrência direta do processo licitatório e podem ser conceituados como **todo e qualquer ajuste entre a Administração Pública e particulares, em que há um acordo de vontade e obrigações recíprocas**.

Deste modo, a Administração consegue envidar maiores esforços para satisfazer as necessidades relativas às atividades-fim e efetua a execução indireta, por meio de contratação de terceiros, de atividades-meio.

PLANEJAMENTO DA CONTRATAÇÃO

É importante que a Administração Pública esteja incorporada à capacidade de antecipação de fatos futuros. Planejar é pensar antecipadamente em termos de objetivos e ações.

Planejar a aquisição de bens e contratação de serviços é essencial, é o ponto de partida para uma gestão efetiva diante da máquina pública, onde a qualidade do planejamento ditará os rumos para uma boa ou má gestão.

No tocante à contratação de bens e serviços de TI, é necessário que o objeto a ser contratado esteja aderente aos instrumentos que permeiam o alinhamento estratégico de Tecnologia da Informação (PETIC e PDSTIC).

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Analisar, nas contratações de bens ou serviços de TI, se o objeto está aderente ao Plano Diretor Setorial de Tecnologia da Informação e Comunicação (PDSTIC) e, caso aplicável, também com o Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC), de forma a auxiliar no cumprimento dos objetivos organizacionais.
- Para contratações que envolvam o desenvolvimento de sistemas, avaliar a possibilidade de separar, em contratos específicos, o desenvolvimento de sistemas de maior complexidade e/ou de maior importância estratégica, com a finalidade de facilitar a mensuração e o gerenciamento das entregas.
- Observar os princípios constitucionais e licitatórios presentes respectivamente no artigo 37 da Constituição Federal (legalidade, impessoalidade, moralidade, publicidade e eficiência) e ater-se às leis vigentes nº 8.666, de 21 de junho de 1993 e a lei nº 14.133, de 1º de Abril de 2021.

PRINCIPAIS OBRIGAÇÕES DA CONTRATADA

As obrigações a serem cumpridas pela contratada devem ser definidas claramente no edital e no contrato, de modo que seja possível verificar, pelos responsáveis do órgão contratante, se a empresa contratada está efetivamente cumprindo com os seus deveres e obrigações.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Contemplar, em edital e no contrato, as obrigações da contratada, especialmente sobre a necessidade de:

■ Fornecer aos contratantes, junto com a proposta comercial ou solicitação de medição, em caso de contrato em vigor, os demonstrativos de formação dos preços unitários referentes a cada serviço e sistema objeto da proposta, em nível de detalhamento que permita a identificação dos recursos produtivos utilizados (insumos), com as respectivas quantidades e custos individuais, vedado o fornecimento de proposta ou solicitação de medição cujos preços sejam formados por agregados de serviços e sistemas.

■ Fornecer aos contratantes todas as informações necessárias para a realização do ateste contratual, definindo também qual a forma e os artefatos em que essas informações serão prestadas.

□ **O fornecimento deverá ser feito dentro dos prazos e padrões previstos, podendo ser recusados os artefatos que não estiverem de acordo com os padrões estabelecidos.**

■ Prover, sempre que requisitado pelo órgão contratante, detalhamento adicional sobre os preços praticados e serviços executados.

■ Atender aos acordos de níveis de serviço (SLA), conforme item 5 desta Orientação, contendo, no mínino, o prazo máximo para solução dos problemas e incidentes.

■ Manter sigilo e tratamento confidencial de dados e informações do órgão setorial contratante, obtidos devido à relação contratual ou execução de serviços.

■ Definir, no início da execução contratual, uma única pessoa como preposto da contratada, que tenha qualificação técnica para gerenciar a execução contratual, sendo que a sua substituição depende de prévia aprovação do substituto pela contratante.

Não compreender, em edital ou no contrato, a possibilidade de a contratada:

■ Subcontratar partes de serviço ou fornecimento, salvo autorização expressa do órgão contratante e nos limites previamente admitidos.

- Renegociar, durante a vigência do contrato, os preços definidos nas cláusulas contratuais, salvo para reequilíbrio econômico-financeiro do contrato, cenário possível em caso de desequilíbrio gerado por evento econômico extraordinário.

Obter cotações com preços unitários já consolidados, para facilitar a análise de economicidade da cotação.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Mensurar o desempenho dos processos utilizados na prestação de serviços, através de indicadores específicos como disponibilidade, capacidade, incidentes, níveis de serviços e segurança da informação, de forma a auxiliar o órgão contratante na verificação do desempenho e tomada de decisões relacionada à execução do contrato. A título exemplificativo, alguns possíveis indicadores poderiam ser:
  - **Relação entre solicitações e incidentes atendida dentro do prazo do acordo de nível de serviço estabelecido;**
  - **Relação entre pontos de função produzidos e o respectivo tempo despendido;**
  - **Relação entre incidentes de segurança de informação e sua criticidade;**
  - **Relação entre disponibilidade dos serviços e sistemas e o respectivo tempo indisponível;**
  - **Relação entre solicitações e incidentes atendidos na central de atendimento e quantidade de pessoal disponibilizado para essas tarefas;**
- Facilitar o acesso às informações relativas ao resultado da medição dos indicadores acordados, através de suas divulgações por iniciativa do próprio contratado, independente de requerimento do contratante.

PRINCIPAIS OBRIGAÇÕES DO CONTRATANTE

e boas práticas

Além das obrigações da contratada, esta Orientação estabelece, também, as principais obrigações e boas práticas do órgão contratante.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Fiscalizar o acordo de nível de serviço estabelecido na contratação;
- Realizar o aceite dos bens, serviços ou sistemas apenas após a efetiva entrega e verificação da quantidade e qualidade, mensurando os resultados efetivos das entregas, individualmente, de cada bem, serviço e sistema objeto do contrato, em nível de detalhamento que permita a identificação das quantidades e preços unitários praticados pelo fornecedor, vedada a formalização de contratos, aceite ou pagamento de bens, serviços e sistemas não individualizados;
- Avaliar na execução contratual se os requisitos técnicos de pessoal exigidos inicialmente estão sendo cumpridos pela contratada, de forma a evitar que os funcionários experientes, usados no início do contrato, sejam movidos rapidamente e substituídos por pessoal menos experiente.
- Evitar, sempre que possível, as seguintes ações por parte da contratante:

  - Realizar pagamentos por mera disponibilização de mão de obra para prestação de serviços ("body shop"). Devendo, portanto, prever em contrato os resultados que deverão ser entregues pela contratada;
  - Praticar atos de ingerência na administração da contratada, através de atos de subordinação ou vinculação hierárquica dos empregados da contratada;
  - Realizar a contratação que tenha por objeto atividades que envolvam tomada de decisão, definição de política de segurança

da informação, coordenação, supervisão ou consideradas estratégicas para o órgão contratante.

QUAIS SÃO AS NOSSAS SUGESTÕES?

Para a contratação de serviços de infraestrutura de redes, servidores e desenvolvimento de sistemas:

- Sempre que possível, deverá existir uma ferramenta que permita ao órgão contratante acompanhar a execução dos serviços realizados pela contratada.
- Sempre que houver infraestrutura e espaço disponíveis, estabelecer que a equipe contratada ficará fisicamente nas dependências do órgão contratante e não da empresa contratada, ressalvados os casos em que a relação custo-benefício não seja vantajosa à Administração.
- Deixar expresso em contrato que, de acordo com o Artigo 4º da Lei Federal n.º 9.609, de 19 de fevereiro de 1998, o contratante tem direito à propriedade de todos os produtos desenvolvidos pela contratada[1].
- Exigir da contratada a documentação das especificações e requisitos dos equipamentos utilizados para suportar a prestação dos serviços, com a finalidade de dimensionar a capacidade atual e facilitar a sua previsão em uma eventual troca de fornecedor.
- Indicar em contrato que as eventuais atualizações e lançamento de versões de softwares estão inclusos no preço da proposta, enquanto as necessidades de manutenção forem remuneradas.
- O contrato deverá indicar que é de responsabilidade da contratada notificar o cliente quando houver falha de segurança conhecida ou descoberta em seu sistema, juntamente com um plano de ação corretiva.

1. O caput do artigo, in verbis: "Salvo estipulação em contrário, pertencerão exclusivamente ao empregador, contratante de serviços ou órgão público, os direitos relativos ao programa de computador, desenvolvido e elaborado durante a vigência de contrato ou de vínculo estatutário, expressamente destinado à pesquisa e desenvolvimento, ou em que a atividade do empregado, contratado de serviço ou servidor seja prevista, ou ainda, que decorra da própria natureza dos encargos concernentes a esses vínculos." (grifo para fins desta OT)

■ Desenhar uma matriz qualitativa comparativa para auxiliar nas decisões. Exemplo:

Cenário / Característica	I	II	III	IV	V
Licenciamento	Atende	Atende	*Não possui*	Atende	Atende
Requisitos do Software	Atende parcialmente	Atende	-	Supera	Supera
Quantidade de usuários	*Não atende*	Atende	-	Atende	Supera
Serviços de Automatização	*Não possui*	*Atende precariamente*	Atende	Atende	Atende
Serviços de Capacitação	*Atende precariamente*	Atende	Atende parcialmente	Atende	Atende
Atendimento da demanda	*Precário*	Parcial	Parcial	Completo	Completo

Figura 1: Comparativo da capacidade de atendimento dos cenários em relação aos requisitos

ACORDO DE NÍVEL DE SERVIÇO

(ANS OU SLA)

O acordo de nível de serviço (ANS ou Service Level Agreement - SLA) é um acordo entre a contratada e a contratante (Órgão Setorial), que estabelece os serviços que a contratada irá prestar, metas e mensuração de desempenho.

O ANS permite que a contratante verifique se o fornecedor está cumprindo o que foi previamente estabelecido, e aplique as sanções definidas no contrato, quando necessário.

Os acordos de nível de serviço podem variar conforme a realidade de cada órgão, podendo envolver disponibilidade, codificação, conformidade de documentos, aderência aos requisitos, cumprimento de prazos, entre outros.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Estabelecer na contratação um acordo de nível de serviço mensurável e que o órgão setorial municipal tenha capacidade de fiscalizá-lo, contendo, no mínino, o prazo máximo para solução de incidentes e dispondo especialmente sobre:
  - **Listagem e descrição do nível de serviço acordado;**
  - **Horário do serviço;**
  - **Definição do que é aceitável (critérios de aceitação);**
  - **Listagem e descrição das não conformidades;**
  - **Implicação de não conformidades (por exemplo, critério de descontos no pagamento);**
  - **Prazo máximo para correção de problemas e incidentes;**
  - **Necessidade de treinamento, consultoria e atendimento ao cliente;**
  - **Caso a contratada seja responsável por responder às reclamações dos usuários sobre a prestação dos serviços, exigir em contrato que uma cópia de todas as reclamações e respostas devem ser encaminhadas à contratante;e**
  - **Penalidades ou retenções de pagamento, conforme aplicável, em caso de descumprimentos.**

CERTIFICAÇÕES E EXPERIÊNCIA DA CONTRATADA

Quando certificações são exigidas das empresas, como o CMMI[2] ou o MPS.BR[3] , os riscos inerentes à contratação são menores para o órgão, pois significa que a empresa possui um determinado nível de maturidade organizacional.

Além disso, a experiência da empresa também auxilia na minimização de riscos por parte da contratante, pelo fato de já possuírem conhecimento relacionados ao objeto do contrato, trazendo consigo lições aprendidas, sabendo como

2. Capability Maturity Model Integration ou Modelo Integrado de Maturidade em Capacitação consiste em um modelo de maturidade de processos de software.

3. Melhoria de Processo de Software Brasileiro consiste em um modelo de maturidade de processos de software.

evitar e corrigir não conformidades, lidar com situações difíceis similares e possuir informações sobre casos de sucesso que elas mesmas participaram. Ou seja, por serem capacitadas e terem experiência, há maiores chances de desenvolverem a solução com a qualidade esperada pelo órgão contratante.

Uma análise semelhante pode ser feita em relação à exigência de profissionais certificados e com experiência. Ou seja, ao se exigir certificações e experiência, os riscos diminuem para a contratante e a qualidade da prestação de serviço tem maior possibilidade de estar de acordo com o esperado.

Além disso, a depender do modelo de contratação, em caso de não exigência dos requisitos acima citados, as empresas tendem a reduzir drasticamente o preço ofertado, não levando em consideração a capacitação dos profissionais (ou a falta de capacitação) para executarem as tarefas exigidas pelo órgão, podendo resultar na baixa qualidade dos serviços e o consequente não atendimento ao interesse público.

Por outro lado, quando certificações e experiências são exigidas na contratação, as opções do mercado acabam ficando mais restritas. Algumas empresas, que também teriam a capacidade de desenvolver a solução com a mesma qualidade de outras certificadas e experientes, não poderiam concorrer.

Deste modo, o órgão contrante precisa estabelecer um parâmetro razoável e justificado entre as exigências estabelecidas e a respectiva restrição de competitividade que porventura possa ocorrer.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Avaliar, por meio de análise de viabilidade e da correlação de fatores como complexidade, criticidade e tecnologia adotadas pela solução, se há necessidade de exigir certificações e experiências para a contratação.

GARANTIA DOS BENS E SERVIÇOS

A garantia dos bens e serviços é de suma importância para diminuir os riscos do órgão público relacionados a vícios ou defeitos que se tornam evidentes somente após o aceite do produto ou encerramento do contrato.

Tem como fundamento legal para o estabelecimento de eventuais garantias os artigos:

> Lei 8.666/93 - Art. 69. O contratado é obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.
>
> Lei 14.133/21 - Art. 119. O contratado será obrigado a reparar, corrigir, remover, reconstruir ou substituir, a suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes de sua execução ou de materiais nela empregados.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Definir, em edital e no contrato, um período razoável de tempo para garantia, período no qual o contratado arcará com quaisquer ônus provenientes de correção de vícios ou defeitos que se tornaram aparentes, inclusive após o aceite do produto ou término do contrato.

CONTRATOS PARA SERVIÇOS EM NUVEM

A Orientação Técnica 009 – Da aquisição dos serviços de computação em nuvem apresenta boas práticas para servir como diretriz de apoio à tomada de decisão na contratação e uso de serviços de computação em nuvem na Administração Municipal.

Em relação ao escopo desta Orientação (diretrizes para contratos relacionados à TI), a Orientação Técnica 009 elenca um conjunto de sugestões e recomendações que tem por objetivo assessorar os órgãos na elaboração do Edital ou Termo de Referência, inclusive relacionando cláusulas segundo o seu grau de importância.

QUANDO AS RECOMENDAÇÕES PASSAM A VALER?

Os procedimentos descritos nesta Orientação Técnica deverão ser aplicados nos procedimentos atuais e futuros, bem como nos contratos futuros e nas prorrogações contratuais, ainda que de contratos assinados antes do início da vigência desta OT.

Esta Orientação Técnica entrará em vigor a partir da sua aprovação pelo CMTIC.

REFERÊNCIAS

Link: https://www.gov.br/compras/pt-br/acesso-a-informacao/legislacao/instrucoes-normativas/instrucao-normativa-no-5-de-26-de-maio-de--2017-atualizada.BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Instrução Normativa Nº 05, de 26 de maio de 2017.

Link: <http://www.planalto.gov.br/ccivil_03/Leis/l8666cons.htm>. BRASIL. Lei N. 8.666, de 21 de junho de 1993. Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências.

Link: <http://www.convergenciadigital.com.br/inf/013463-2017-9%20serprodataprev.pdf>. TRIBUNAL DE CONTAS DA UNIÃO (TCU). TC 013.463/2017-9 – Relatório de Auditoria do Tribunal de Contas da União. Brasília, 2017. p.88. Acessado em 02.03.2023

Link: https://www.gartner.com/document/3823169/key-insight?ref=ddisp&refval=200963335&qid=4eb040f4efe92df6d380f-dcd797cf564. Depende de cadastramento para acessar

Link: <http://www.gartner.com>.Acessado em 02.03.2023

- Use These 10 Contracting Steps to Dramatically Reduce Your Application Implementation Project Overruns. 1º de novembro de 2017.
- Outsourcing Contract Research Index. 2016
- Outsourcing Contract — Fees and Payment Terms. 30 de setembro de 2015
- Contract Review Checklist. 6 de dezembro de 2017

Link: https://repositorio.enap.gov.br/bitstream/1/5564/2/M%-C3%B3dulo%202%20-%20Planejamento%20da%20Contrata%C3%A7%C3%A3o%20de%20TIC..pdf - Escola Nacional de Administração Pública - Planejamento da Contratação de TIC – Módulo 2. Brasília, 2020Acessado em 02.03.2023

[OT 012]
MODELOS DE CONTRATAÇÃO E MÉTRICAS DE DIMENSIONAMENTO DE SISTEMAS

Visa considerar modelos de contratação como o paradigma básico a ser utilizado pela Administração com a finalidade de mensurar e remunerar os bens e atividades que fazem parte de uma solução de Tecnologia da Informação.

PRINCIPAIS MODELOS DE CONTRATAÇÃO

Para o escopo desta Orientação, podemos considerar modelos de contratação como o paradigma básico a ser utilizado pela Administração com a finalidade de mensurar e remunerar os bens e atividades que fazem parte de uma solução de Tecnologia da Informação.

Dentre os modelos mais relevantes, destacam-se:

CONTRATO POR PREÇO FECHADO

Consiste no modelo de contratação em que o preço é acordado previamente pelas partes, de acordo com o escopo especificado pela contratante. Suas principais características são:

- **A principal dificuldade é a definição e a rigidez do escopo, pois se não feita corretamente pode resultar em um produto diferente do esperado ou que não atende às expectativas;**
- **O valor do desenvolvimento poderá não corresponder com exatidão ao esforço a ser empreendido, já que as empresas costumam estimá-lo no começo da especificação do produto;**
- **É interessante contratar por este modelo quando houver um desenvolvimento com data de entrega definida e que não possa ser postergada sem prejuízos à Administração.**

CONTRATO POR HOMEM-HORA:

Consiste na contratação da mão de obra, remunerada pelas horas que o profissional contratado utilizou para realizar o serviço. Suas principais características são:

- **Este modelo de contratação também deverá ter o escopo definido, ainda que a estimativa total de esforço não seja precisa;**
- **Maior flexibilidade quanto ao escopo do que a contratação por preço fechado. Por exemplo, se houver um aumento no escopo, haverá um aumento nas horas trabalhadas e na remuneração da contratada;**
- **Devido à maior flexibilidade, por vezes o produto final diverge do estimado inicialmente; por isso, é importante ter o controle das solicitações de desenvolvimento;**
- **Este modelo deve ser evitado, pois potencializa a redução da eficiência dos esforços de desenvolvimento, uma vez**

que a remuneração é em função das horas gastas; logo, quanto maior a demora no desenvolvimento, maior será a remuneração da contratada;

- **Muitas vezes um contrato remunerado por homem-hora acaba por se confundir com a mera disponibilização de mão de obra para prestação de serviços ("body shop"), o que deve ser evitado. Devendo, portanto, prever em contrato os resultados que deverão ser entregues pela contratada.**

CONTRATO BASEADO EM MÉTRICAS

Consiste na contratação baseada em métricas previamente definidas, que propiciam uma medida efetiva do serviço prestado e produto entregue. As métricas mais utilizadas são ponto de função (PF) e unidade de serviço técnico (UST), que serão detalhadas nesta Orientação. Suas principais características são:

- **Possibilita uma efetiva medição dos serviços realizados pela contratada (pagamento por resultado), ainda que as metodologias atualmente existentes não sejam imunes a falhas ou lacunas;**
- **Permite maior flexibilidade quanto ao escopo do que a contratação por preço fechado, com maior assertividade na relação produto/esforço.**

Desta forma, podemos resumir as principais caraterísticas dos modelos mencionados anteriormente:

Modelo de Contratação	Vantagens	Desvantagens
Preço Fechado	Custo definido previamente.	Pouca flexibilidade para mudanças.
Homem-hora	Maior flexibilidade para mudanças.	Dificuldade de mensurar os serviços efetivamente entregues e potencial redução de eficiência.
Métricas de dimensionamento	Maior flexibilidade para mudanças e mensuração efetiva das entregas realizadas no contrato.	Exigência de profissionais capacitados.

Tabela 1: Modelos de Contratação

Para desenvolvimento de sistemas utilizando metodologias ágeis, é possível adotar uma variante do modelo de contratação por preço fechado, na qual é definido previamente o custo de uma *sprint* de desenvolvimento. A quantificação do custo pode ser feita de diversas formas, incluindo o uso de *story points* ou de *ideal days* (dias ideais)[4] . Vale ressaltar que, para desenvolvimento ágil, via de regra, se fixa o custo, a qualidade e o prazo, variando-se o escopo.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Avaliar, com base nas características elencadas neste documento, o modelo que melhor se adequa às necessidades do órgão contratante para a contratação de determinada solução ou prestação de serviços de Tecnologia da Informação;
- Evitar realizar pagamentos por mera disponibilização de mão de obra para prestação de serviços ("body shop"), devendo, portanto, prever em contrato os resultados que deverão ser entregues pela contratada;
- Utilizar métricas quando da contratação, seja por meio da adoção de um modelo de contratação baseado em métricas ou, no caso de contratações baseados em homem-hora, realizar o controle da execução por meio de Ordens de Serviço (OS) ou por meio de projetos baseados em UST e/ou pontos de função, com entregáveis objetivos e preços fechados.

  ■ A utilização de métricas para contratação de serviços de Tecnologia da Informação se compatibiliza com o entendimento dos órgãos de controle, especialmente no tocante à remuneração por resultados, como a Súmula 269 do Tribunal de Contas da União:

  > Nas contratações para a prestação de serviços de tecnologia da informação, a remuneração deve estar vinculada a resultados ou ao atendimento de níveis de serviço, admitindo-se o

pagamento por hora trabalhada ou por posto de serviço somente quando as características do objeto não o permitirem, hipótese em que a excepcionalidade deve estar prévia e adequadamente justificada nos respectivos processos administrativos. (TCU, Súmula 269).

MÉTRICAS PARA DESENVOLVIMENTO DE SISTEMAS

E PRESTAÇÃO DE SERVIÇOS DE INFRAESTRUTURA

Métricas, no escopo da Tecnologia da Informação, possibilitam quantificar alguns indicadores como tamanho, esforço, custo e prazo das tarefas necessárias à realização de determinada atividade.

Os principais objetivos de sua utilização são:

- **Remunerar contratos de prestação de serviços de Tecnologia da Informação;**
- **Aumentar a exatidão das previsões sobre custos e prazos dos projetos;**
- **Reduzir os defeitos e outros problemas do produto;**
- **Reduzir os custos e prazos do projeto;**
- **Identificar necessidades de novos investimentos;**

Dentre as métricas mais utilizadas, destacam-se: Linhas de Código, Ponto de Função, Pontos de Caso de Uso, e Unidade de Serviço Técnico.

Linhas de Código consiste numa contagem de linhas de codificação existentes em uma determinada funcionalidade ou aplicação. É uma medida extremamente simples e objetiva. Todavia, é dependente da tecnologia (linguagem de programação) a ser utilizada e da forma em que o código é escrito.

Ponto de função é a unidade de medida que tem por objetivo tornar a medição independente da tecnologia utilizada para a construção do software. Ou seja, ela busca medir o que o software faz, e não como ele foi construído.

Basicamente, podemos seguir quatro modelos distintos para o uso e cálculo da técnica de pontos de função: IFPUG (International Function Point Users GrouP), NESMA (Netherlands Software Metrics Association) e Roteiro de métricas do SISP (Sistema de Administração dos Recursos de Tecnologia da Informação), do Governo Federal ou Guia de Métricas de software FINEP.

A técnica de análise de ponto de função (APF) propõe-se a mensurar:

- **A funcionalidade que o usuário solicita e recebe; e**
- **O desenvolvimento e a manutenção de software de forma independente da tecnologia utilizada para sua implementação.**

A figura a seguir ilustra o procedimento de contagem de pontos de função:

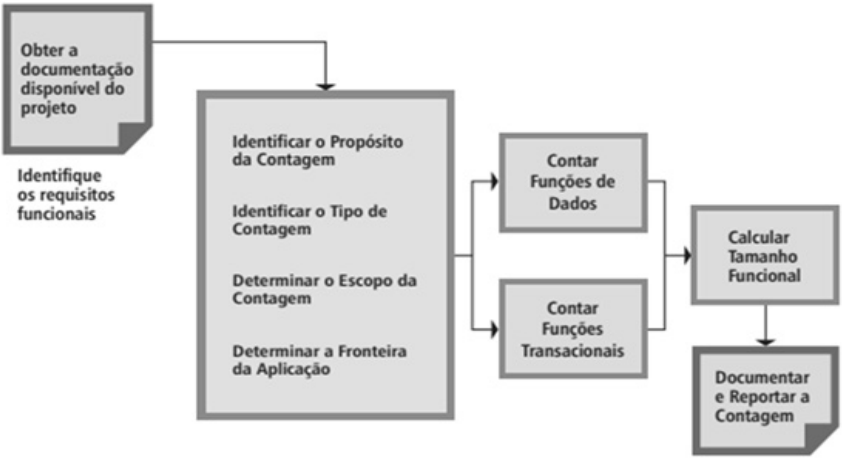


Figura 2: o procedimento de contagem de pontos de função

Para cumprir os seus objetivos, o processo de contagem de pontos de função deve ser:

- **Simples o suficiente para minimizar o trabalho adicional envolvido no processo de medição; e**
- **Uma medida consistente entre vários projetos da organização.**

Não obstante, a métrica de análise de pontos de função (APF) possui as seguintes desvantagens:

- **A contagem não é intuitiva, devendo ser realizada por pessoas capacitadas na técnica de APF; e**
- **Seu cálculo envolve apenas o que o usuário entende como funcionalidade (ponto de vista do usuário), não mensurando, por exemplo, requisitos não funcionais (desempenho, usabilidade, segurança, etc).**

No tocante às atividades nas quais a métrica de pontos de função não se aplica diretamente, como requisitos não funcionais, é fundamental definir claramente no edital quais seriam estes requisitos a serem atendidos pela contratada,

uma vez que eles impactam diretamente no esforço e, consequentemente, no custo do projeto.

Seguem abaixo alguns tipos de requisitos não funcionais, a título meramente ilustrativo, que poderiam ser mencionados nos editais:

- **Usabilidade: a solução deve atender aos requisitos dos Padrões Web em Governo Eletrônico (e-PWG) – Cartilha de Usabilidade; a aplicação deve ter help on-line de sistema, tela e campo (sensível a contexto); a aplicação deve ser disponibilizada nos idiomas Português, Espanhol e Inglês.**
- **Técnicos: a aplicação deve funcionar adequadamente nos navegadores: Internet Explorer 7.0 ou superior e Mozilla Firefox 3.0 ou superior; a solução deve ser desenvolvida em linguagem Java com banco de dados PostgreSQL; para o desenvolvimento da solução, deve ser utilizado preferencialmente um dos seguintes frameworks Java: Demoiselle, Jaguar e MDArt; a solução deve atender aos requisitos do e-PWG; deve utilizar as ferramentas AWSTATS e Google Analytics para gerar estatísticas de acesso.**
- **Segurança: a aplicação deve realizar controle de segurança dos dados de acordo com politica de backup definida em conformidade com a norma ISO/IEC 27002. - Acessibilidade: a solução deve ser aderente ao Modelo de Acessibilidade de Governo Eletrônico (e-MAG).**
- **Performance: o tempo de resposta da aplicação não deve exceder 10 segundos; a solução deve suportar até 1.000 acessos simultâneos.**
- **Interoperabilidade: a solução deve ser aderente aos Padrões de Interoperabilidade de Governo Eletrônico (e-PING).**

Como alternativa à mensuração de requisitos não funcionais, uma das desvantagens que a técnica de pontos de função não consegue medir diretamente, o IFPUG desenvolveu a técnica de Pontos de SNAP, sendo muito semelhante à contagem de Pontos de Função. Não obstante, é raro seu uso em órgãos da Administração Pública.

Além disso, para outras atividades que não sejam diretamente dimensionadas pelo ponto de função ou que o seu uso não seja muito adequado, como simples adequação de layout em uma página, é possível prever formas alternativas de contagem como a Unidade de Serviço Técnico (UST), que será demonstrada posteriormente nesta Orientação.

Pontos de Caso de Uso, por sua vez, é uma métrica proposta como uma adaptação do método de Pontos de Função para aplicação em projetos orientados a objeto, a partir dos casos de uso levantados na fase de requisitos.

No entanto, possui a restrição de só ser aplicado em projetos que utilizam casos de uso e, para a análise da complexidade dos casos de uso, as definições propostas não são muito objetivas e dependem muito da forma como os casos de uso são escritos e detalhados.

A Unidade de Serviço Técnico (UST) (ou denominações correlatas) é uma métrica que mede o esforço para executar determinada atividade previamente definida, equivalendo, geralmente, a uma hora de serviço técnico especializado.

Ela deve necessariamente estar associada a um catálogo de serviços, onde será detalhada a relação entre a atividade a ser executada e a quantidade equivalente de USTs antecipadamente definida e os resultados esperados. Em geral, a quantidade de USTs de cada atividade pode ser alterada de acordo com a complexidade da tarefa.

Idealmente, o catálogo de serviços deve ser taxativo, de forma a prever o maior número possível de serviços que serão utilizados durante a execução contratual.

Entretanto, na prática, durante a execução contratual, surgirão necessidades não abrangidas pelos itens previstos inicialmente no catálogo de serviços.

Como alternativa, é possível prever em edital e no contrato

que, na falta de estimativa relativa a determinado serviço, a contratada e a contratante, em consenso, utilizarão a analogia com itens similares já existentes no catálogo, bem como a aferição empírica através de projeto piloto de duração reduzida e acompanhada pela contratante.

É possível, ainda, a utilização de fator de complexidade ou criticidade tanto para a quantificação das USTs como para os pontos de função equivalentes à determinada atividade, quando previamente definido em contrato, que resultará em uma majoração dos valores inicialmente previstos quando se tratar de serviços urgentes, críticos, não seja padronizado ou demande um maior esforço no atendimento pela contratada, como no caso de demandas que devam ser atendidas em finais de semana, feriados e fora do horário comercial ou que demandem maior esforço pela contratada.

A aplicação do fator de ajuste deve ser prerrogativa exclusiva da contratante e não deve ser utilizado para compensar falta de experiência ou capacidade dos profissionais alocados pela contratada.

Além de poder ser utilizada no desenvolvimento de sistemas, podem constar do catálogo de serviços diversas atividades de suporte, DevOps[5] , infraestrutura e auxiliares, como: administração de servidores, banco de dados, segurança da informação, mapeamento de processos, dentre outros.

Por fim, algumas métricas podem ser utilizadas apenas em prestação de serviços de desenvolvimento de sistemas (linhas de código, pontos de caso de uso e pontos de função), enquanto outras podem ser utilizadas para serviços de infraestrutura ou auxiliares (UST ou homem-hora).

5. DevOps é um termo que deriva da junção das palavras "desenvolvimento" (development) e "operações" (operations), sendo uma prática de engenharia de software que possui o intuito de unificar o desenvolvimento de software e a operação de software, tendo como principal característica a automação e monitoramento em todas as fases da construção do software, da integração, teste, liberação para implantação e gerenciamento de infraestrutura.

Parâmetros para Cálculo de UST:

- **Identificar o agregador;**
- **Identificar o cenário que será medido;**
- **Identificar se o cenário depende de BPM/Serviço/ECM**
- **Determinar quantidade de regras de negócio, apresentação e integrações do cenário medido – para cálculo de interface.**

Fórmula: UST = Comp * BPM * ECM * SERV * PI

Onde:

COMP = Fator relativo à complexidade do cenário

Complexidade	Descrição	Fator COMP
Baixa	Telas compostas com componentes simples (combos, caixas de texto, check box, rádio, etc.)	1
Média	Telas que possuem "dual lists" e "grids"	1,25
Alta	Telas que apresentem recursos como diagramas (gantt, tree, etc.) e gráficos diversos.	1,5

Tabela 2: principais características das métricas de dimensionamento

- **BPM = Fator que indica relação com fluxo de BPM**
- **ECM = Fator que indica relação com fluxo de ECM**
- **SERV = Fator que indica implementação de algum serviço**

Fator	Não possui / não contém	Possui / Contém
Baixa	1	1,15
Média	1	1,6
Alta	1	1,15

- **PI = Quantidade de pontos por Interface (obtido através da soma dos pontos de regras de negócio, apresentação e integração do cenário). Fórmula: PI = PRN + PRA + INT**

Qtd. Regras de negócio	Pontos PRN
Nenhuma regra	0
1 a 3 regras	13
4 a 6 regras	39
7 ou mais regras	77

Qtd. Regras de negócio	Pontos PRA
Nenhuma regra	0
1 a 5 regras	13
6 a 10 regras	39
11 ou mais regras	77

Qtd. Regras de negócio	Pontos INT
Nenhuma Integração	0
1 a 2 Integrações	13
3 a 4 Integrações	39
5 ou mais Integrações	77

A tabela a seguir resume as principais características das métricas de dimensionamento apresentadas nesta Orientação Técnica, além da sua possível utilização:

Métrica	Vantagens	Desvantagens	Utilização
Linhas de Código	Objetiva Pode ser automatizada	Dependente de tecnologia (linguagem de programação) e da forma de escrita do código	Desenvolvimento de Sistemas
Pontos de função	Independente de Tecnologia Ponto de vista do usuário	Difícil mensuração Não mede requisitos não funcionais	Desenvolvimento de Sistemas
Pontos de caso de uso	Utiliza dos próprios documentos de requisitos como base	Pode ser utilizada apenas em sistemas que utilizam casos de uso Depende de como o caso de uso foi escrito (subjetivo)	Desenvolvimento de Sistemas
Unidade de Serviço Técnico (UST)	Fácil mensuração	Depende de um bom catálogo de serviços	Desenvolvimento de Sistemas e Infraestrutura

Tabela 3: principais características das métricas de dimensionamento

Com a finalidade de auxiliar os Órgãos Setoriais em contratações públicas baseadas nas técnicas e modelos expostos nesta Orientação, poderá o Órgão Central elaborar documentos auxiliares, publicando-os no Portal de Governança.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Buscar capacitação e atualização permanentes em métricas e procedimentos que permitam melhorar a contratação, desenvolvimento, implantação e/ou manutenção dos sistemas de Tecnologia da Informação.
- Buscar capacitação e atualização periódicas para os servidores envolvidos na fiscalização e gestão dos contratos de Tecnologia da Informação.
- Independente da métrica escolhida, o órgão deve adotar no desenvolvimento de sistemas:
  - Iterações curtas e entregas frequentes, observando a metodologia adotada e a complexidade do software, para que haja diminuição nos riscos das entregas e melhor acompanhamento contratual;
  - Metodologia e boas práticas de análise e gerenciamento de requisitos;
  - Previsão de sanção ou retenção de pagamento em caso de descumprimentos contratuais; e
  - Previsão de prazos para a realização das atividades a serem desenvolvidas.
- Sempre que possível, deixar expresso em edital e no contrato que não há garantia de consumo mínimo da métrica utilizada para fins de remuneração, de forma a trazer uma maior liberdade ao órgão municipal no tocante ao uso dos serviços contratados apenas quando efetivamente necessários à Administração.
- Abster-se de realizar pagamentos adicionais por atividades a serem realizadas pela contratada que sejam inerentes às suas responsabilidades, como reuniões ou outros custos operacionais da contratada que já fazem parte dos encargos do próprio contrato.
- Determinar em edital e em contrato a métrica a ser utilizada cujas características possibilitem avaliar adequadamente o objeto do contrato.

- É válida a utilização de mais de uma métrica em conjunto para o mesmo objeto, ou o uso de forma alternativa que não esteja prevista neste documento, desde que sua aplicação permita uma efetiva aferição dos resultados entregues pelo contratado.
- Quando a métrica escolhida não conseguir dimensionar todas as atividades necessárias à contratação, considerar a possibilidade de utilizar mais de uma forma de medição ou realizando equivalências para fins de precificação.

- **Por exemplo, requisitos não funcionais, que não são mensuráveis pela métrica de Pontos de Função, poderiam ser medidos por Unidade de Serviço Técnico (UST), caso previsto no instrumento contratual.**
- **No caso de utilização da métrica de Unidade de Serviço Técnico (UST), contemplar em edital e no contrato, obrigatoriamente, o catálogo de serviços relacionando as tarefas com as quantidades predefinidas de USTs.**
- **Contemplar em edital e no contrato, para o caso de utilização da métrica de pontos de função, o método de contagem escolhido (IFPUG, NESMA ou Roteiro do SISP ou Guia de Métricas de software FINEP) e que servirá de base para o cálculo do dimensionamento.**

QUAIS SÃO AS NOSSAS SUGESTÕES?

- **Na contratação de serviços de desenvolvimento de novos sistemas, analisar a viabilidade de adotar as métricas de Pontos de Função ou Unidade de Serviço Técnico (UST), adotando, preferencialmente, esta última.**
- Na prestação serviços de sustentação dos sistemas existentes, a métrica de Unidade de Serviço Técnico (UST) possui uma melhor relação custo-benefício quando comparada com outras métricas. Todavia, a métrica de Pontos de Função também pode ser utilizada nestas atividades.

- Na contratação de serviços de infraestrutura, a adoção da métrica de Unidade de Serviço Técnico (UST) para mensuração do trabalho realizado pode ser mais interessante, uma vez que a contagem é mais intuitiva e objetiva em comparação à utilização de homem-hora.
- Ao optar pelo uso de medição por UST, pode ser interessante utilizar as fórmulas apresentadas no Capitulo 2 - Parâmetros para Cálculo de UST.
- Ao optar pelo uso de pontos por função, buscar identificar o(s) tipo(s) de projeto(s) de software e definir métricas através de parâmetros estabelecidos para contagem de pontos. Seguem exemplos que apresentam diferentes níveis de complexidade:
  - Projeto de Desenvolvimento;
  - Projeto de Melhoria;
  - Projetos de Migração de Dados;
  - Manutenção Corretiva;
  - Mudança de Plataforma;
  - Atualização de Versão;
  - Manutenção em Interface;
  - Adaptação em Funcionalidades sem Alteração de Requisitos Funcionais;
  - Atualização de Dados;
  - Desenvolvimento, Manutenção e Publicação de Páginas Estáticas de Intranet, Internet ou Portal.

MÉTRICAS PARA CONTROLE DE PROJETO

E QUALIDADE DO DESENVOLVIMENTO DE SISTEMAS

Especialmente para o desenvolvimento de sistemas utilizando metodologias ágeis, é importante que as entregas aconteçam de forma rápida, mas sem a perda de qualidade.

Para isso, o uso de métricas para avaliar a qualidade, atreladas eventualmente a SLA (Acordo de Nível de Serviço) e outros dispositivos contratuais, pode ser bastante interessante para que se tenha formas objetivas de verificar que o desenvolvimento esteja acontecendo da forma como planejado.

Para fins desta Orientação Técnica, três métricas básicas são apresentadas, sem prejuízo de outras métricas que os Órgãos Setoriais possam adotar em seus projetos de desenvolvimento:

Razão entre o número de stories completados e o número de stories planejados para cada sprint;

- **Esta métrica não avalia apenas a velocidade, mas também a qualidade da organização da sprint avaliada, em termos de escolha e detalhamento das stories que poderiam ser desenvolvidas e completadas dentro do prazo previsto, estando diretamente correlacionado com a granularidade das stories e com a eficácia do grupo que trabalha nelas.**
- **O Órgão Setorial poderá utilizar esta métrica também como uma forma de detectar gargalos nos esforços de desenvolvimento e qualidade.**

Taxa de execução bem-sucedida de casos de testes;

- **Esta métrica tenta avaliar o processo de verificação das mudanças e seu impacto na estabilidade operacional. Uma execução bem-sucedida de teste significa que as alterações de código estão sendo validadas, além de indicar que o próprio processo de validação está funcionando.**

- **O Órgão Setorial pode utilizar esta métrica para avaliar se as manutenções evolutivas, preventivas e corretivas de sistemas estão acontecendo como deveriam. A redução nos valores desta métrica pode indicar um excesso de velocidade no desenvolvimento, no caso de metodologias ágeis, ou uma falha no processo de qualidade.**

Taxa de Escape (Escape rate).

- **A taxa de escape é uma métrica que consiste em contar a quantidade de bugs que são encontrados em cada release após a sua subida em ambiente de produção. Esta é uma das métricas mais críticas, pois conversa diretamente com a efetividade do desenvolvimento e da qualidade.**
- **Uma elevação na taxa de escape é um potencial indicativo de que o processo de desenvolvimento e/ou da qualidade necessita de atenção imediata do Órgão Setorial.**

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Avaliar a adoção das métricas propostas, sem prejuízo de outras métricas possíveis, para medir e melhorar a qualidade do desenvolvimento, especialmente no caso de contratação de terceiros.
  - A avaliação poderá ser feita apenas por Órgãos que possuem equipe de Tecnologia da Informação e Comunicação do Órgão com integrantes formalmente capacitados em métricas e qualidade de software.

QUANDO AS RECOMENDAÇÕES PASSAM A VALER?

Os procedimentos descritos nesta Orientação Técnica deverão ser aplicados nos procedimentos atuais e futuros, bem como nos contratos futuros e nas prorrogações contratuais, ainda que de contratos assinados antes do início da vigência desta OT.

Esta Orientação Técnica entrará em vigor a partir da sua aprovação pelo CMTIC.

REFERÊNCIAS

Link: <https://www.governodigital.gov.br/documentos-e-arquivos/Roteiro%20de%20Metricas%20de%20Software%20do%20SISP%20-%20v2.0.pdf>. Brasil. Ministério do Planejamento, Desenvolvimento e Gestão. Roteiro de Métricas de Software do SISP – Versão 2.3. Brasília: 2018 - Acessado em 02.03.2023.

Link: <https://www.microsoft.com/en-us/research/publication/the-art-of-testing-less-without-sacrificing-quality/> Microsoft. The Art of Testing Less without Sacrificing Quality. 2015.- Acessado em 02.03.2023.

Link: https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/*/KEY:ACORDAO-COMPLETO-29379/NUMACORDAOINT%20asc/0 - TCU. Acórdão n° 786/2006 – Plenário. Relator: Ministro Augusto Sherman Cavalcanti. Acessado em 02.03.2023

Link: http://www.finep.gov.br/images/licitacoes/2017/Consulta012017/II_GuiaDeMetricasDeSoftware.pdf - Guia de Métricas de Software – FINEP - Acessado em 02.03.2023.

Link: https://www.gov.br/governodigital/pt-br/contratacoes/portaria-sgd-me-no-5651-de-28-de-junho-de-2022 - Acessado em 02.03.2023.

[OT 013]
DIRETRIZES BÁSICAS DE SEGURANÇA DA INFORMAÇÃO

CONSIDERAÇÕES INICIAIS

A Segurança da Informação deve permear todos os campos de conhecimento em termos de Tecnologia da Informação e Comunicação, sendo calcada em três grandes pilares, quais sejam: pessoas, políticas/procedimentos e mecanismos tecnológicos.

Além disso, ela compreende diversas dimensões que influenciam, em todo ou em parte, as diversas iniciativas em Tecnologia da Informação e Comunicação. Para fins desta Orientação Técnica, são adotadas as seguintes dimensões, sem prejuízo de outras possibilidades a serem estabelecidas por cada Órgão Setorial para consecução de seus processos de negócio:

- **Confidencialidade: propriedade de não estar disponível ou não ser revelado para indivíduos, entidades ou processos não autorizados;**
- **Integridade: propriedade de completude e fidedignidade;**
- **Disponibilidade: propriedade de estar acessível e usável para atender tempestivamente à demanda de uma pessoa, processo, ou entidade autorizada;**
- **Autenticidade: propriedade de que uma pessoa, organização, entidade, documento ou informação é de fato o que ela diz ser;**
- **Irretratabilidade: também conhecida como não-repúdio, é a capacidade de provar a ocorrência de determinado evento ou ação, bem como provar a sua autoria ou responsabilidade;**
- **Rastreabilidade: capacidade de detectar a ocorrência de determinado evento ou ação, prover caracterização adequada do fato e determinar a sua autoria;**
- **Confiabilidade: propriedade de obter comportamentos e resultados de forma prevista e consistente;**
- **Utilidade: propriedade de agregar ou gerar valor em termos organizacionais; e**
- **Consciência: ato e estado de conhecimento, internalização e adoção de determinada informação como tendo valor relevante em termos pessoais e/ou organizacionais.**

Em termos de gestão, a Segurança da Informação é baseada em Elementos Fundamentais e dividida em diversas Áreas de Gestão.

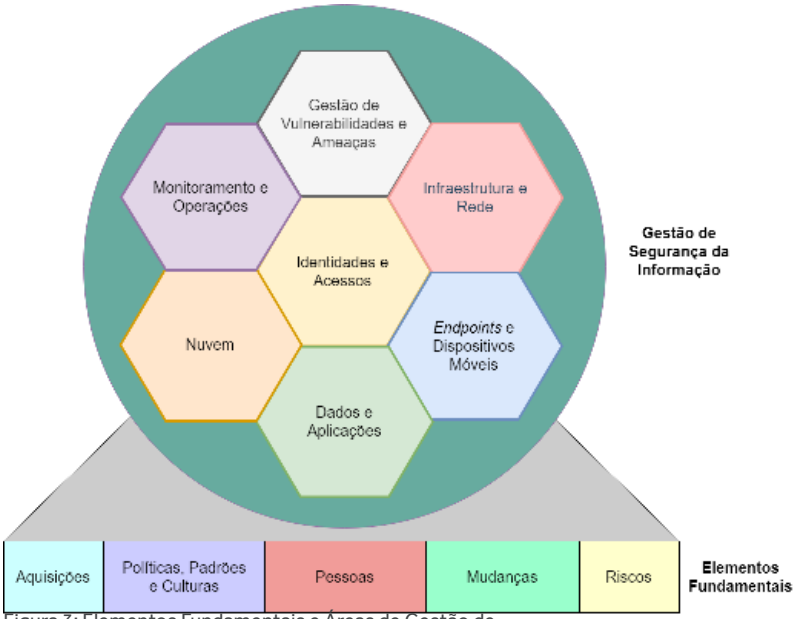


Figura 3: Elementos Fundamentais e Áreas de Gestão de Segurança da Informação. (adaptado do Gartner)

Os Elementos Fundamentais são:

- **I. Aquisições;**
- **II. Políticas, Padrões e Culturas;**
- **III. Pessoas;**
- **IV. Mudanças;**
- **V. Riscos;**

As Áreas de Gestão são:

- **I. Gestão de Vulnerabilidades e Ameaças;**
- **II. Monitoramento e Operações;**
- **III. Infraestrutura e Rede;**
- **IV. Identidades e Acessos;**

- **V. Nuvem;VI. Endpoints e Dispositivos Móveis;**
- **VII. Dados e Aplicações;**

ELEMENTOS FUNDAMENTAIS

de segurança da informação

A boa gestão das aquisições é um componente essencial também em termos de Segurança da Informação, pois permite benefícios como:

- **I. mitigação de vulnerabilidades de segurança;**
- **II. redução de complexidade e heterogeneidade em equipamentos e endpoints;**
- **III. maior estabilidade nos componentes de TI;**
- **IV. menores custos de suporte;**
- **V. tempos menores de resposta e resolução.**

O estabelecimento e a implementação de um programa de Segurança da Informação, com a definição de políticas e padrões, assim como o fomento de uma cultura positiva em termos de Segurança da Informação, é crucial para a efetividade das iniciativas.

A geração de consciência positiva nas pessoas envolvidas fortalece um dos três grandes pilares da Segurança da Informação, possibilitando inclusive uma redução de custos, financeiros e/ou administrativos, na implementação de mecanismos de Segurança da Informação, além de naturalmente mitigar potenciais vulnerabilidades.

A promoção de cultura corporativa de Segurança da Informação é fundamental e contempla iniciativas originárias dos níveis hierárquicos mais altos (top-down), incluindo o suporte da Alta Administração e o seu protagonismo como bons exemplos, e iniciativas com origem nas bases (grassroot), que engloba a conscientização e educação da força de trabalho.

A estabilidade e o insight são fatores relevantes para a efetividade da Segurança da Informação. Estabilidade significa que as mudanças ao ambiente são bem pensadas, racionais e sob alguma forma de governança que a controle. Já o insight permite que a organização conheça, compreenda e reaja aos componentes e atividades dentro do ambiente, tais como pessoas, aplicações e sistemas.

A prática de arquitetura empresarial (Enterprise Architecture) como framework estratégico para os processos é interessante, inclusive, em termos de Segurança da Informação, para dar previsibilidade e estabilidade ao ambiente e se tornar subsídio para a definição de padrões e para desenvolvimento consistente e repetível, bem como a elaboração de mapas de caminho.

As pessoas são fatores fundamentais para a efetividade da Segurança da Informação, de forma que se torna necessário ter um ambiente propício à adoção de comportamentos adequados em termos de Segurança da Informação.

A conscientização é a chave para o sucesso da Segurança da Informação. É importante estimular o engajamento das pessoas de forma adequada e com visibilidade das iniciativas. Nesse contexto, é interessante trabalhar com líderes para dar o exemplo e comunicar o que se espera das pessoas, assim como obter colaboração para coletar e disseminar informações.

A Segurança da Informação preconiza que as pessoas precisam ter não só a liberdade e autonomia necessárias para executar o serviço, mas também o conhecimento para tomar decisões mais corretas.

A Segurança da Informação prescreve que há a necessidade das pessoas terem a liberdade de falhar, ao mesmo tempo em que elas devem reconhecer, se apropriar e responder rapidamente a essas falhas. Uma cultura que ajude

as pessoas que contribuam ao programa de Segurança da Informação permite detecção mais rápida de problemas e fornece oportunidades para evitar que eventuais problemas aumentem de tamanho/complexidade.

A gestão apropriada da mudança é primordial para se manter a estabilidade, especialmente em um contexto de mudanças extremamente rápidas, como é o caso da tecnologia da informação e comunicação, objetivando, entre outras coisas, evidenciar a aprovação e a rastrebailidade da mudança.

No âmbito desta Orientação Técnica, define-se mudança como uma alteração de processo/procedimento e/ou de arquitetura de software.

A gestão da mudança contempla naturalmente as questões de segurança.

A gestão apropriada de riscos é imprescindível para a Segurança da Informação, pois baliza a tomada de decisões, inclusive em termos de apetite de risco.

A gestão de riscos envolve iniciativas como análise de contexto, avaliação, tratamento e monitoramento dos riscos, comunicação e revisão dos mecanismos implantados.

Em um primeiro nível, a gestão de riscos especifica a necessidade de adoção de controles, com a subsequente definição de níveis aceitáveis e de processos de controle.

Para fins desta Orientação Técnica, a gestão de riscos engloba também a gestão de incidentes, que compreende processos como:

- **a. plano para determinar quais sensores dos controles estão sendo usados para detectar incidentes, quando e como;**
- **b. processo gerencial de resposta para deter, recuperar e mitigar um incidente;**
- **c. processo de revisão para, no mínimo, evitar que o problema ocorra novamente ou, pelo menos, melhorar a resposta e mitigação em caso de nova ocorrência.**

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Definir e publicizar, no mínimo, no âmbito do próprio Órgão Setorial, políticas internas que descrevam uso aceitável, entendido como sendo a diligência do usuário em compreender que os ativos de informática da Prefeitura são ativos corporativos (e não pessoais) e atuar para que haja adequada distinção no uso e armazenamento dos dados corporativos e pessoais, bem como requisitos básicos de segurança para, posteriormente, desenvolver mais padrões e especificações como parte da melhora do processo de gestão de riscos.
- Investir em capacitações técnicas de Segurança da Informação atualizadas e apropriadas para o corpo técnico de tecnologia da informação e comunicação, inserindo-as no planejamento de capacitação em tecnologia da informação e comunicação do Órgão Setorial.
- Aprimorar a gestão de ativos de microinformática, com a implantação de um inventário atualizado, preferencialmente de modo automatizado, e seguindo o disposto em outras Orientações Técnicas.
- Aprimorar a gestão de redes corporativas sem fio, protegendo adequadamente por meio de mecanismos como autenticação de usuários e criptografia de tráfego.
- Aprimorar a gestão de sistemas, incluindo-se eventuais nuvens e ambientes de IoT (internet das coisas), e seguindo o disposto em outras Orientações Técnicas.
- Aprimorar a gestão de licenças e patches de software, com a implantação de um inventário atualizado, preferencialmente de modo automatizado, e seguindo o disposto em outras Orientações Técnicas.
- Aprimorar a gestão de dados, incluindo códigos-fonte, com a implantação de repositórios apropriados e métodos de classificação de informações, e seguindo o disposto em outras Orientações Técnicas.

- Aprimorar a gestão de usuários e permissões de acessos, com a implantação e execução do ciclo de vida de usuários e acessos, e seguindo o disposto em outras Orientações Técnicas.
- Aprimorar a gestão de aquisições, buscando inclusive obter maior padronização dos ativos, em compasso com o inciso I do Artigo 15 da Lei 8.666/1993, e seguindo o disposto em outras Orientações Técnicas.
- Realizar a gestão da qualidade da Segurança da Informação, com o desenvolvimento e aplicação de indicadores, bem como avaliação periódica de ambientes e sistemas chaves em termos de Segurança da informação.
- Incluir questões de segurança na gestão da mudança.
- Estabelecer controles e definir os respectivos processos de controle, incluindo a definição de níveis de aceitação.
- Considerar necessidades de compliance regulatório por força de outros normativos, tais como a Lei Federal 13.709/2018 (Lei Geral de Proteção de Dados) e a Lei Federal 12.965/2014 (Marco Civil da Internet), e refleti-las nos controles adotados.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Se a gestão da mudança não incluír inicialmente as questões de segurança, começar com abordagens pontuais, simples e fáceis de serem adotadas.
- Estabelecer pontes com outras atividades e unidades da organização, tais como: recursos humanos, administrativo/financeiro e as unidades responsáveis pelos processos de negócio do Órgão Setorial. Construir relacionamentos com outras unidades facilita angariar suporte a desenvolvimentos futuros de boa gestão integrada de riscos, bem como o fomento mais rápido das práticas fundamentais em termos de Segurança da Informação.

- Planejar e executar um programa de conscientização de Segurança da Informação, de maneira a estimular comportamentos aceitáveis dos usuários em termos de Segurança da Informação.
- Definir questões relativas à autoridade e ownership de riscos e informações para que a Alta Administração do Órgão Setorial realize a sua implantação.

ÁREAS DE GESTÃO

DE SEGURANÇA DA INFORMAÇÃO

A Gestão de Vulnerabilidades e Ameaças é uma prática básica em termos de Segurança da Informação, visto que uma das atuações mais intuitivas na área seria exatamente a identificação de ameaças, a eliminação de vulnerabilidades e o uso de controles para mitigar ameaças residuais.

- **I. A priorização de iniciativas de mitigação ou remediação é parte da gestão.**
- **II. A busca por ameaças mais específicas e avançadas é algo a ser considerado por Órgãos Setoriais com maior nível de Maturidade.**

A área de Monitoramento e Operações envolve a parte operacional da implementação de controles e detecção/eliminação/mitigação de ameaças.

A avaliação da qualidade das operações é uma atividade relevante, uma vez que não há uma ferramenta única capaz de mitigar todas as possibilidades e certamente nenhuma ferramenta é capaz de eliminar todas as ameaças.

O processo de monitoramento poderá começar como sendo pontual, para então passar para ocasional/periódico e chegar enfim ao estado desejado, que é o monitoramento contínuo.

A Infraestrutura e Rede contêm frequentemente os ativos mais valiosos em termos de tecnologia da informação e comunicação e, portanto, necessitam de proteção adequada, especialmente se o Órgão Setorial possuir um data center ou similar.

A segurança da rede envolve a proteção de ambientes virtualizados como IaaS e outras formas de acesso remoto.

O controle de Identidades e Acessos é, muitas vezes, um dos objetivos mais claros e imediatos de Segurança da Informação e permeia todas as demais áreas, direta ou indiretamente.

A Nuvem precisa ser tratada de forma diferenciada em termos de Segurança da Informação, uma vez que existem diversas formas de contratação e uso, impactando na implementação e operação dos controles de segurança.

A contratação e/ou uso da nuvem traz consigo questões não técnicas, especialmente questões de caráter legal/regulatório, que precisam ser levadas em consideração.

Os Endpoints e Dispositivos Móveis são um elemento de extrema relevância em qualquer arquitetura ou infraestrutura de tecnologia da informação e comunicação.

A questão do BYOD (Bring Your Own Device) é um desafio a ser tratado, considerando-se por um lado a sua conveniência e baixo custo, e por outro lado os riscos de se ter dados do Órgão Setorial em equipamentos e ambientes fora do seu controle direto.

A segurança das Aplicações trata tanto da segurança em termos de desenvolvimento quanto de execução, incluindo a proteção dos Dados que utilizam. Os Dados propriamente ditos são geralmente os ativos mais valiosos a serem protegidos e medidas devem ser tomadas para sua proteção, para fins de inserção/atualização/exibição/eliminação, processamento, armazenamento e transmissão/transferência.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Observar as Orientações Técnicas e correlatas e normativos em vigor afeitos para entender e atender, dentro do que for pertinente, as respectivas Recomendações e Sugestões.

POLÍTICAS BÁSICAS

DE SEGURANÇA DA INFORMAÇÃO

Esta Orientação Técnica estabelece uma política básica de Segurança da Informação em três níveis: o Nível 0 é voltado aos Órgãos Setoriais que não possuem nenhuma política de Segurança da Informação, o Nível 1 se dirige aos que já implantaram o Nível 0 e, por fim, o Nível 2 é voltado aos Órgãos Setoriais que já alcançaram o Nível 1.

Deve-se ressaltar que a política descrita nesta Orientação se limita apenas ao que se entende ser o mínimo indispensável, estando muito longe ainda do ideal. É fundamental que cada Órgão sempre busque enriquecer, expandir e aprimorar a Segurança da Informação dentro da sua organização, para além do disposto nesta Orientação Técnica.

NÍVEL 0

O Nível 0 é voltado aos Órgãos Setoriais que não possuem maturidade suficiente para desenvolver atividades mais específicas de Segurança da Informação, seja por falta de conhecimento, seja por falta de equipe, ou ainda por ser um Órgão Setorial recém-criado e, portanto, ainda em processo de estruturação.

Nesse caso, é importante que o responsável pela Tecnologia da Informação e Comunicação tenha pelo menos algumas informações rudimentares em mãos. Naturalmente, isso

está longe de ser suficiente, necessitando que haja esforços para aumentar a maturidade do Órgão Setorial em termos de Tecnologia da Informação, de forma a avançar nos níveis da Segurança da Informação.

O Nível 0 exige as seguintes medidas:

Área de Gestão	**Medidas a serem implementadas**
Gestão de Vulnerabilidades e Ameaças	-o-
Monitoramento e Operações	-o-
Infraestrutura e Rede	Limitar o uso de contas de administrador ou similares, bem como privilégios administrativos de acesso/execução, de forma que apenas as pessoas que realmente precisem tenham acesso a essas contas e/ou privilégios. Alterar todas as senhas padrão de infraestrutura e de rede para uma senha mais segura, gerido pelo responsável pela tecnologia da informação e comunicação do Órgão Setorial.
Identidades e Acessos	Implantar e manter processos de gestão de identidades e acessos, incluindo a parte de provisionamento, alteração e exclusão. Verificar, junto ao Integrador Estratégico e/ou ao prestador de serviços de infraestrutura, que são aplicados critérios de senha, para se ter senhas adequadamente fortes. Restringir as contas privilegiadas de usuário, tais como as contas de administrador, root e equivalentes, para que apenas os usuários que necessitam tais contas por necessidade de serviço, ou usuários que sejam servidores de carreira ou especialização em tecnologia da informação, possam ter permissão de uso de tais contas. Definir processos de concessão e revogação de acesso, podendo incluir a necessidade de assinatura de um termo de responsabilidade.

Nuvem	Considerar, como padrão, que os dados na nuvem devem estar armazenados em território brasileiro.
Endpoints e Dispositivos Móveis	Verificar, junto ao Integrador Estratégico e/ou ao prestador de serviços de infraestrutura, que está acontecendo a aplicação de patches do sistema operacional e de outras aplicações, para eliminar vulnerabilidades conhecidas. Verificar, junto ao Integrador Estratégico e/ou ao prestador de serviços de infraestrutura, que há a proteção de endpoints, seja por meio de uma solução integrada ou por meio de um conjunto de soluções, incluindo pelo menos um antivírus. Verificar, junto ao Integrador Estratégico e/ou ao prestador de serviços de infraestrutura, que foram implantados para rede wireless, configurando no mínimo o protocolo WPA2. Alterar todas as senhas padrão das contas de administrador ou equivalentes para uma senha mais segura, gerida pela equipe de tecnologia da informação e comunicação do Órgão Setorial. Implantar um sistema de gestão de ativos para gerir os endpoints.
Dados e Aplicações	Localizar onde estão os dados mais críticos armazenados pelo Órgão Setorial e, se estiverem armazenados em equipamentos pessoais, ter pelo menos uma cópia atualizada periodicamente em um repositório corporativo do Órgão. Implantar infraestrutura e rotinas básicas de backup de dados, considerando a Orientação Técnica sobre o tema. Verificar, junto ao Integrador Estratégico e/ou ao prestador de serviços de infraestrutura, que há controles de acesso às bases de dados do Órgão Setorial, de forma que o acesso seja estritamente em função das necessidades de serviço.

NÍVEL 1

O Nível 1 se destina aos Órgãos Setoriais que já iniciaram um processo de desenvolvimento e amadurecimento da sua equipe de Tecnologia de Informação e Comunicação. O objetivo é começar a munir a equipe com conhecimentos e ferramentas para atuarem de forma mais presente.

Além do Nível 0, o Nível 1 exige também as seguintes medidas:

Área de Gestão	Medidas a serem implementadas
Gestão de Vulnerabilidades e Ameaças	-o-
Monitoramento e Operações	-o-
Infraestrutura e Rede	Implantar medidas de segurança física para proteger no mínimo a infraestrutura principal de tecnologia da informação e comunicação do Órgão Setorial, incluindo[6]: ■ **Porta com chave/cadeado que esteja efetivamente operacional.** ■ **Claviculário ou equivalente para guardar as chaves, incluindo as chaves dos racks.** ■ **Limitação do acesso físico à infraestrutura principal apenas às pessoas que efetivamente trabalham com os ativos localizados na mesma.**
Identidades e Acessos	Definir papéis para padronizar os conjuntos de permissões de acesso, ao invés de definir acessos para cada usuário, documentando os papéis definidos e mantendo a documentação no repositório de dados corporativo do Órgão Setorial. Aplicar critérios de senha, para se ter senhas adequadamente fortes.
Nuvem	-o-

Endpoints e Dispositivos Móveis	Gerir a aplicação de patches do sistema operacional e de outras aplicações, para eliminar vulnerabilidades conhecidas. ■ **Avaliar também a possibilidade de utilizar o servidor WSUS do Integrador Estratégico ou até mesmo ter um servidor WSUS interno ao Órgão Setorial, de forma a evitar congestionamento de rede.** Implantar a proteção de endpoints, seja por meio de uma solução integrada ou por meio de um conjunto de soluções, incluindo pelo menos: ■ **Anti-malware, incluindo antivírus;** ■ **Firewall;** ■ **Filtro para navegação Web, que pode ser implantado tanto por meio de uma solução centralizada quanto por meio de add-ons de navegadores;** ■ **Detector de comportamento suspeito/anômalo.** Implantar e manter mecanismos de segurança para rede wireless, configurando no mínimo o protocolo WPA2.
Dados e Aplicações	Implantar controles de acesso às bases de dados do Órgão Setorial, de forma que o acesso seja estritamente em função das necessidades de serviço. Se o Órgão realizar o desenvolvimento de aplicações, incluir como requisito não funcional a exigência de não inserir segredos (senhas, tokens etc.) no código-fonte, exceto para fins meramente de testes. Se o Órgão realizar o desenvolvimento de aplicações, implantar controle de versão e gestão de repositório de código. Se o Órgão realizar o desenvolvimento de aplicações, incluir no desenvolvimento a geração de logs de auditoria.

6. Por "infraestrutura principal" entende-se o ambiente que se designa informalmente como a "sala de servidores", contendo os servidores e/ou os ativos de rede principais. Excluem-se os *data centers* (salas-cofre e infraestrutura associada), pois as exigências nesse caso são diferenciadas e muito mais rigorosas.

NÍVEL 2

O Nível 2 deve incorporar, ainda que em parte, da abordagem baseada em riscos. Para que isso possa ser realizado, o Órgão Setorial deverá ter pelo menos uma pessoa da equipe de tecnologia de informação e comunicação que tenha recebido capacitação formal em análise e gestão de riscos, preferencialmente o líder da equipe de tecnologia de informação e comunicação.

Além do Nível 1, o Nível 2 exige também as seguintes medidas:

Área de Gestão	Medidas a serem implementadas
Gestão de Vulnerabilidades e Ameaças	Utilizar ferramentas automatizadas para conduzir, de forma periódica, avaliação básica de vulnerabilidade em sistemas de alto valor que o Órgão disponibiliza na internet.
Monitoramento e Operações	Definir e documentar processos básicos de continuidade de negócios e recuperação de desastres para pelo menos um evento negativo de impacto crítico.
Infraestrutura e Rede	Implantar mecanismos de detecção de ativos não identificados e/ou não autorizados na rede interna. Implantar e manter um ou mais firewalls para controlar o tráfego de rede, especialmente se o Órgão Setorial tiver um link direto para a internet. Implantar e manter uma ou mais VPNs (rede privada virtual), especialmente se o Órgão Setorial utilizar acesso remoto, incluindo a conexão a algum ambiente IaaS. Implantar e manter um sistema de detecção e/ou prevenção a intrusões de rede, preferencialmente como parte de um firewall ou de um produto de gestão unificada de ameaças (UTM). Planejar, implantar e documentar a segmentação/ zoneamento de rede.
Identidades e Acessos	-o-

Nuvem	Investir em capacitação para ganhar conhecimento na avaliação do melhor modelo de contratação/implantação, além de conhecimentos para realizar a contratação em si. Considerar, como padrão, que os dados na nuvem devem estar armazenados em território brasileiro. ■ **No caso do Órgão Setorial ter um líder de TI com capacitação formal em Gestão de Riscos e/ou uma unidade formalmente constituída de Segurança da Informação, o Órgão poderá armazenar seus dados na nuvem fora do território nacional, mediante análise de risco e justificativa.**
Endpoints e Dispositivos Móveis	Implantar um sistema e/ou um processo de gestão de licenças de software, incluindo um processo contínuo de adequação e atualização planejada das licenças. Realizar um processo de hardening (melhoria de robustez dos endpoints) de acordo com boas práticas conhecidas, tais como: ■ **Utilizar guias, checklists ou benchmarks amplamente utilizadas pelo mercado para ter um ponto de partida de realização de *hardening*[7];** ■ **Utilizar imagens atualizadas para instalar nos endpoints, se possível já após um processo de hardening da imagem;** ■ **Limitar os privilégios das contas de administrador ou root local e/ou as pessoas com acesso a essas contas.**
Dados e Aplicações	Se o Órgão realizar o desenvolvimento de aplicações, mapear as dependências da segurança da aplicação em termos de infraestrutura. Se o Órgão realizar o desenvolvimento de aplicações, incorporar um mecanismo ou processo de teste de segurança de aplicações dentro da etapa de testes do ciclo de desenvolvimento de aplicações. Se o Órgão disponibiliza aplicações para a internet que são hospedadas dentro da sua própria infraestrutura, implantar uma WAF (Web Application Firewall).

7. Alguns exemplos possíveis:
https://nvd.nist.gov/ncp/repository
https://iase.disa.mil/stigs/Pages/a-z.aspx
https://github.com/nsacyber/Windows-Secure-Host-Baseline
http://www.buffalo.edu/content/dam/www/ubit/docs/guidance-documents/appendix-a-server-security-checklist.pdf

Para o caso específico do Nível 2, o líder da unidade formalmente constituída para gerir a tecnologia de informação e comunicação do Órgão Setorial poderá estabelecer um plano de adoção gradual das medidas descritas, considerando-se questões de caráter técnico, de pessoal e orçamentário/financeiro.

Em caso de ter alguma prática ou controle listados acima que exijam tecnologia e/ou processo que o Órgão Setorial ainda não detém, o líder poderá realizar e executar um planejamento, refletido no Plano Diretor Setorial de Tecnologia da Informação e Comunicação e limitado à disponibilidade orçamentária, para adquirir e/ou desenvolver tal tecnologia, bem como desenvolver e internalizar os processos necessários.

Em termos de Escala de Maturidade, a aplicação comprovada da política em Nível 1 habilita o Órgão Setorial a pleitear a medalha de bronze em Política de Segurança da Informação.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Para um Órgão Setorial sem nenhuma política de Segurança da Informação publicada ou publicizada, implantar a política em Nível 0 desta Orientação, seguindo-se o checklist disponível no Anexo.
- Para um Órgão Setorial que já implantou a política em Nível 0, buscar a implantação do Nível 1.
- Para um Órgão Setorial que já implantou a política em Nível 1, buscar a implantação planejada e gradual do Nível 2, considerando-se as capacidades e necessidades técnicas, de pessoal e de orçamento.
- Se o Órgão já alcançou o Nível 2, buscar aprimorar e expandir os seus controles de segurança para melhor gestão da Segurança da Informação.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Automatizar os procedimentos de dimensionamento e alocação de infraestrutura.
- Incorporar os requisitos de segurança dentro do processo de desenvolvimento ou do termo de referência de aquisição da aplicação.

QUANDO AS RECOMENDAÇÕES PASSAM A VALER?

Os procedimentos descritos nesta Orientação Técnica deverão ser aplicados nos procedimentos atuais e futuros, bem como nos contratos futuros e nas prorrogações contratuais, ainda que de contratos assinados antes do início da vigência desta OT.

Esta Orientação Técnica entrará em vigor a partir da sua aprovação pelo CMTIC.

REFERÊNCIAS

Guia: Wonham, Mike. Building the Foundations for Effective Security Hygiene. Gartner, 2018. Publicado em 08 de agosto de 2018.

ANEXO

CHECKLIST NÍVEL 0

ITEM	OK?
As contas padrão de usuário não são contas de administrador, nem de administrador local ou equivalente.	
As contas de administrador dos servidores ou dos computadores que atuam como tal são geridas apenas pela equipe de Tecnologia de Informação e Comunicação do Órgão Setorial.	

Restringir as contas privilegiadas de usuário, tais como as contas de administrador, root e equivalentes, para que apenas os usuários que necessitam tais contas por necessidade de serviço, ou usuários que sejam servidores de carreira ou especialização em tecnologia da informação, possam ter permissão de uso de tais contas.	
As contas de acesso para os ativos de infraestrutura e de rede são geridas apenas pela equipe de Tecnologia de Informação e Comunicação do Órgão Setorial, pelo Integrador Estratégico ou pelo prestador de serviços de infraestrutura.	
Todas as senhas padrão dos ativos de infraestrutura e de rede que estiverem sob a gestão da equipe de Tecnologia de Informação e Comunicação do Órgão Setorial estão alteradas para uma senha não padrão, preferencialmente com o uso de caracteres e números no mínimo.	
Todas as senhas padrão dos ativos de infraestrutura e de rede que estiverem sob a gestão da equipe de Tecnologia de Informação e Comunicação do Órgão Setorial são alteradas periodicamente, pelo menos a cada três anos ou sempre que for necessário, para uma outra senha não padrão, preferencialmente com o uso de caracteres e números não utilizados na senha anterior.	
Existe um aceite formal dos servidores, admitido o uso de meio eletrônico/digital, explicitando o conhecimento e a concordância com as Políticas de Segurança implantadas no Órgão Setorial.	
É executada uma varredura periódica, no mínimo anualmente, para identificar os usuários que não são mais utilizados (ex: usuários dos servidores que já foram exonerados).	
É executado um procedimento periódico, no mínimo anualmente, para bloquear e/ou eliminar os usuários inativos, isto é, os usuários que não são mais exonerados.	
Existe um documento corporativo (ou equivalente) atualizado periodicamente com os sistemas utilizados no Órgão Setorial e os respectivos procedimentos para solicitação de acesso.	
O documento corporativo (ou equivalente) atualizado com os sistemas está armazenado em um repositório corporativo, e não pessoal, do Órgão Setorial.	

Existe um procedimento corporativo para concessão de permissões de acesso a usuários, registrando-se os pedidos de concessão, preferencialmente por meio eletrônico.	
Existe um procedimento corporativo que define formalmente quem é o autorizador da concessão de permissão de acesso, sendo que o autorizador não pode ser o próprio usuário, salvo no caso do Secretário, Secretário Adjunto, Subprefeito, Chefe de Gabinete e equivalentes.	
Existe um procedimento corporativo que define formalmente os critérios de exclusão de permissão de acesso, incluindo no mínimo os casos de bloqueio/exclusão do usuário e a remoção em caráter fático do servidor.	
É executada uma varredura e adequação periódicas das permissões concedidas a cada usuário, excluindo-se as permissões que não sejam estritamente necessárias ao cumprimento das atividades atuais do usuário.	
Existe um documento formal do Integrador Estratégico e/ou do prestador de serviços de infraestrutura, admitido o uso de documento eletrônico/digital, explicitando que são adotados critérios e procedimentos para se ter senhas adequadamente fortes para os usuários e ativos do Órgão Setorial que são geridos pelas entidades supra.	
Existe um documento formal do Integrador Estratégico e/ou do prestador de serviços de infraestrutura, admitido o uso de documento eletrônico/digital, explicitando que são adotados políticas de aplicação de patches do sistema operacional e de outras aplicações, para eliminar vulnerabilidades conhecidas.	
Existe um documento formal do Integrador Estratégico e/ou do prestador de serviços de infraestrutura, admitido o uso de documento eletrônico/digital, explicitando que existem medidas para a proteção dos endpoints do Órgão Setorial geridos pelos mesmos, seja por meio de uma solução integrada ou por meio de um conjunto de soluções, incluindo pelo menos um antivírus.	

Existe um documento formal do Integrador Estratégico e/ou do prestador de serviços de infraestrutura, admitido o uso de documento eletrônico/digital, explicitando que existem medidas para a proteção da rede wireless do Órgão Setorial gerida pelos mesmos, configurando no mínimo o protocolo WPA2 para segurança.	
Existe um sistema de gestão de ativos implantado, operacional e em utilização no Órgão Setorial para gerir os ativos de microinformática (essencialmente desktops, notebooks e similares).	
Existe um procedimento corporativo, de preferência formal, que permite à equipe de Tecnologia de Informação e Comunicação do Órgão Setorial localizar e copiar para o repositório corporativo, de ofício, os dados corporativos armazenados em equipamentos pessoais, especialmente para o caso de remoção, aposentadoria e/ou exoneração iminente do servidor.	
Existe um procedimento corporativo implantado, junto com a infraestrutura necessária, para a execução de rotinas básicas de backup de dados, considerando a Orientação Técnica sobre o tema.	
Existe um documento formal do Integrador Estratégico e/ou do prestador de serviços de infraestrutura, admitido o uso de documento eletrônico/digital, explicitando que existem medidas para limitar o acesso direto à base de dados do Órgão Setorial, de forma que o acesso seja realizado estritamente em função das necessidades de serviço.	

[OT 014]
ADEQUAÇÃO DO ESPAÇO FÍSICO DE TIC

AMBIENTE FÍSICO DE TECNOLOGIA DA INFORMAÇÃO

O ambiente de trabalho está diretamente ligado ao desempenho dos colaboradores de uma empresa ou instituição, sendo um dos fatores que podem ajudar a melhorar a produtividade dos agentes envolvidos e, consequentemente os resultados alcançados pela organização.

Há diversos estudos e normas técnicas que regulam vários dos itens do local de trabalho, tais como equipamentos, mobiliário e condições do ambiente, sendo que alguns deles dizem respeito ao ambiente físico de Tecnologia da Informação e Comunicação - TIC, variando desde a ergonomia do local de trabalho até as características específicas das estruturas de TIC.

Todavia, sabe-se que alguns dos itens tratados para a adequação do ambiente de trabalho possuem ligação direta com outros setores da organização, além de lidar com fatores externos regulamentadores, tais como a zeladoria do local e normas de higiene e segurança.

Além disso, fatores financeiros ou orçamentários poderão prejudicar ou até mesmo incapacitar o desenvolvimento de algumas modificações relativas a um bom ambiente de trabalho.

Esta Orientação Técnica traz direcionamentos para alguns dos espaços físicos relacionados com Tecnologia da Informação considerados mais relevantes por um grupo de trabalho composto por representantes voluntários de vários órgãos setoriais integrantes do Sistema Municipal de Tecnologia da Informação e Comunicação – SMTIC.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Adaptar o ambiente existente, visando proporcionar conforto, segurança e bem-estar aos agentes públicos para o desempenho das atividades relacionadas à Tecnologia da Informação e Comunicação.
- Prever espaço apartado do ambiente de trabalho para equipamentos categorizados como inservíveis e em fase de desfazimento.
- Prever espaço seguro para armazenar o estoque e novos equipamentos de TIC.

SALA DE SERVIDORES

Uma sala de servidores é o espaço físico onde se reúnem os equipamentos que armazenam os arquivos e dados que trafegam pela rede de computadores de uma empresa ou organização. Essa sala, além de estar em um local seguro onde apenas seja acessível a pessoas autorizadas, também deve manter os elementos ambientais, tais como calor e umidade, sob controle.

É interessante destacar que os servidores têm como função atender todo o Órgão Setorial e fazem parte da espinha dorsal da rede de tecnologia da informação do Órgão. Por esse motivo, sua localização física deve ser estratégica dentro do layout da organização, tanto por motivos de segurança, como pelo cabeamento estruturado que conectará os servidores aos ativos de rede e, por sua vez, a todos os computadores e demais equipamentos.

O planejamento de uma sala de servidores é importante para a construção de um ambiente seguro para as informações

pertinentes ao Órgão Setorial, buscando a confidencialidade, integridade e disponibilidade dos dados da instituição.

Ressalte-se que esta seção não trata dos requisitos para um data center e/ou sala cofre, que possuem exigências muito mais rigorosas.

Ressalte-se também que o atendimento da Sala de Servidores a esta Orientação Técnica, ainda que em sua integralidade, não é condição suficiente para que eventuais servidores, físicos ou virtuais, localizados em tal sala estejam aptos a hospedarem aplicações do Órgão Setorial. A hospedagem de aplicações em ambiente interno próprio do Órgão demanda outros requisitos que estão além do escopo desta Orientação Técnica.

ESTRUTURA

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- A sala de servidores deve ter um tamanho apropriado de acordo com o número e tamanho dos equipamentos que vai acomodar.
- Usar prateleiras, armários de metal ou racks apropriados para a instalação das máquinas físicas.
- Adotar mecanismos para evitar ou mitigar oscilações de tensão, que podem comprometer ou até mesmo inutilizar os ativos de TI.
- Instalar os equipamentos de forma a otimizar o acesso a eles para fins de manutenção e evitar armazenar equipamentos e outros objetos de forma a prejudicar ou até mesmo impedir o acesso.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Ter a sala de servidores em localização que facilite a distribuição e a organização da rede.
- Evitar salas com janelas, e caso haja janelas e incidência de luz solar, utilizar alguma proteção, como por exemplo uma película reflexiva específica, para diminuir a luminosidade e o calor absolvido.
- Ao planejar o espaço de uma sala de servidores, lembrar-se de deixar um espaço extra, caso seja necessário ampliar sua rede.
- Uma prática vantajosa e alternativa à anterior é elevar o piso da sala de servidor. Assim, todo o cabeamento pode ser realizado por baixo, proporcionando melhor ventilação e organização do ambiente, além de reduzir a probabilidade de rompimento de cabos e desconexões acidentais.
- Outra prática vantajosa é instalar teto falso, para facilitar a passagem de cabeamento. Tanto no caso de piso elevado quanto teto falso, é necessário cuidar para que os cabos estejam devidamente protegidos, inclusive em termos de estática.
- Instalar os roteadores e switches de borda em uma área de baixo tráfego e/ou de tráfego controlado.
- Optar por um piso (ex: piso emborrachado) que evite a criação de carga estática, que pode ser prejudicial aos equipamentos.
- Evitar o uso de carpete dentro da sala de servidores uma vez que revestimentos como o carpete podem ser inflamáveis, acumular calor e pó, além de poder interferir no funcionamento dos equipamentos através de carga estática.
- Ter uma rede elétrica estabilizada, utilizando-se no mínimo nobreaks como prevenção.

CLIMATIZAÇÃO

Deve-se priorizar e contemplar no planejamento da sala de servidores um sistema de refrigeração constante de ar condicionado, incluindo aberturas e unidades que removam a umidade existente no local, uma vez que um alto índice de calor e umidade podem levar a falhas de hardware e, em alguns casos, a perda de dados. O excesso de calor pode causar o superaquecimento das máquinas.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Escolher uma sala em que possa ser instalado um aparelho de ar condicionado de conforto, com drenagem externa à sala dos servidores.
- O aparelho de ar condicionado deve possuir a potência de refrigeração em BTUs adequada para a área em metros quadrados da sala de servidores.
- O aparelho de ar condicionado deve permitir a regulagem da temperatura interna da sala de servidores.
- A sala de servidores deve ter um índice controlado de umidade.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Manter a temperatura ideal na entrada de ar dos equipamentos críticos de TI entre 18° C e 27° C com umidade relativa do ar entre 40 e 55%.
- Monitorar os indicadores dos equipamentos e da temperatura da sala de servidores.

ACESSO

Contar com uma sala de servidores de livre acesso ou em local de passagem não é recomendado, por questões de segurança. Os equipamentos de uma sala de servidores processam dados de importância para o órgão setorial e devem ser tratados da maneira adequada. Os funcionários da limpeza, por exemplo, raramente recebem a correta instrução para realizarem a limpeza no local, a qual deve ser acompanhados por uma pessoa da equipe de TIC do Órgão Setorial, pois algum procedimento incorreto pode ocasionar danos irreparáveis.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Reservar a sala de servidores como sendo de uso exclusivo do setor de TIC do órgão setorial, não sendo permitido manter equipamentos ou objetos de qualquer outro setor.
- Implantar procedimentos de segurança para o acesso à sala. Assim, somente os profissionais autorizados terão essa concessão.
- A sala de servidores deve ter pelo menos uma tranca com chave como proteção física.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Instalar sistemas para segurança física dentro da sala do servidor e nas portas.
- Utilizar câmeras de segurança dentro e fora de salas de servidores para prevenir e auxiliar nos casos de sinistro.

NORMAS

Existem normas que definem um padrão para a instalação da sala de servidor. Para prédios comerciais, o padrão atual é o ANSI/TIA 568-D, de 2017, que especifica algumas normas para a tipologia de rede, a instalação do cabeamento e outros pontos importantes.

SEGURANÇA FÍSICA

Com o objetivo de prevenir o acesso físico não autorizado, danos e interferências nos recursos de processamento das informações, é necessário tomar certas medidas de segurança quanto ao espaço físico utilizado pelos agentes de TIC do órgão setorial, sem prejuízo dos controles já apresentados na seção anterior para a Sala de Servidores.

CONTROLES DE ENTRADA FÍSICA

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.

SEGURANÇA

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- O órgão setorial deve possuir um claviculário ou equipamento equivalente para manter e guardar as chaves dos equipamentos de TIC, tais como racks e sala de servidores.

Proteger o cabeamento de energia e de telecomunicações

que transportam dados ou fornece suporte aos serviços de informação, de forma a eliminar ou mitigar interceptação, interferência ou danos.

A remoção de ativos e equipamentos de tecnologia da informação não deve ser feita sem autorização prévia e/ou o acompanhamento de um servidor da área de tecnologia da informação do Órgão Setorial.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Avaliar se o ambiente físico está adequado às normas de segurança de trabalho emitidas pelo Ministério do Trabalho e Emprego no tocante a proteção contra incêndio (NR 24).

LOCAIS DE TRABALHO

MESAS E BANCADAS

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Para trabalho manual sentado ou que tenha de ser feito em pé, as bancadas, mesas, escrivaninhas e os painéis devem proporcionar ao trabalhador condições de boa postura, visualização e operação e devem atender aos seguintes requisitos mínimos:
  - compatibilidade com o tipo de atividade;
  - ter características dimensionais adequadas.
- Para Órgãos que fazem a manutenção de hardware de computadores, possuir bancadas específicas para a manutenção de microcomputadores.

- Manter mesas e bancadas minimamente limpas e organizadas, de forma a ter acesso rápido e seguro às ferramentas e instrumentos de trabalho, bem como ter espaço suficientemente seguro para trabalhar.
- Separar os itens novos dos itens usados, mas utilizáveis. Descartar os itens não utilizáveis.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Avaliar a compatibilidade, com relação ao trabalho desempenhado, das mesas e bancadas em termos de altura e características da superfície.
- Avaliar a dimensão das mesas e bancadas de forma a permitir movimentação adequada.
- Organizar a disposição das eletrocalhas, spiradutos, cabos de rede e telefônicos, de forma a não prejudicar o trânsito das pessoas e de modo a reduzir o risco de causar acidentes e/ou danos.
- Para Órgãos que fazem a manutenção de hardware de computadores, possuir bancadas específicas para a manutenção de microcomputadores com manta antiestática e uso de pulseiras antiestáticas.
- Avaliar outros critérios de adequação conforme normas de segurança de trabalho.

ASSENTOS

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Adotar como requisitos mínimos de conforto e segurança:
  - altura ajustável à estatura do trabalhador e à natureza da função exercida;

- borda frontal arredondada;
- encosto com forma levemente adaptada ao corpo para proteção da região lombar.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Para as atividades em que os trabalhos devam ser realizados sentados, a partir da análise ergonômica do trabalho, poderá ser exigido suporte para os pés, que se adapte ao comprimento da perna do trabalhador.

QUANDO AS RECOMENDAÇÕES PASSAM A VALER?

Os procedimentos descritos nesta Orientação Técnica deverão ser aplicados nos procedimentos atuais e futuros, bem como nos contratos futuros e nas prorrogações contratuais, ainda que de contratos assinados antes do início da vigência desta OT.

Esta Orientação Técnica entrará em vigor a partir da sua aprovação pelo CMTIC.

REFERÊNCIAS

Documento: ABNT, Associação Brasileira de Normas Técnicas. NBR 13962:2018 - Móveis para escritório - Cadeiras - Requisitos e métodos de ensaio.

Documento: ABNT, Associação Brasileira de Normas Técnicas. NBR 13967:2011 – Móveis para escritório - Sistemas de estação de trabalho - Classificação e métodos de ensaio.

Documento: ABNT, Associação Brasileira de Normas Técnicas. NBR 14565:2013 - Cabeamento estruturado para edifícios comerciais e data centers.

Documento: ANSI/TIA-568-B Commercial Building Telecommunications Cabling – Generic Telecommunications Cabling for Costumer Premises - (Norma para Cabeamento de Telecomunicações em Edifícios Comerciais – Cabeamento de Telecomunicação).

Link: http://www.mte.gov.br - BRASIL, Ministério do Trabalho e Emprego. Normas Regulamentadoras de Segurança e Medicina do Trabalho – Acessado em 03.03.2023.

- NR 17 Ergonomia
- NR 23 Proteção Contra Incêndios.
- NR 24 Condições Sanitárias e de Conforto nos Locais de Trabalho.

Guia: Gartner, Inc. "Create a Catalog of Activity-Based Spaces in the Digital Workplace to Improve the Employee Experience". GOTTA, Mike; ROZWELL, Carol. Publicado em 10/02/2017.

Documento: ISO/IEC 11801:2002 2ND Edition Generic Cabling for Customer Premises.

Recomendação: ASHRAE (American Society of Heating, Refrigerating and Air Conditioning Engineers).

[OT 015]
ADEQUAÇÕES DA EQUIPE DE TIC

COMPOSIÇÃO DA EQUIPE DE TI

É inegável que a tecnologia tornou-se indispensável no cotidiano das pessoas e nos setores da sociedade, inclusive na administração pública que, assim como o setor privado, vê a necessidade de alinhar os objetivos estratégicos do negócio com a sua capacidade de lidar e operar com a Tecnologia da Informação e Comunicação (TIC), e para isso necessita de profissionais capacitados para as operações relacionadas.

Devido ao impacto gerado, aumenta-se a demanda por todos os serviços prestados pelas unidades de TI, serviços esses que envolvem diversos tipos de atividades quer ligadas com acesso a informação, armazenamento de dados, conectividade à internet, disponibilidade de rede, suporte técnico, gestão de aplicações, dentre muitas outras ações desenvolvidas sob o guarda-chuva de TIC.

Os princípios da eficiência e economicidade influenciam diretamente aspectos como a quantidade de pessoas trabalhando nos diversos setores da PMSP. Consequentemente, devido à atuação, a área de TIC, que exige capacidades técnicas específicas e mão de obra especializada, também busca ser eficiente adequando à quantidade de pessoas alocadas em seu funcionamento de acordo com suas qualificações técnicas.

Entretanto, no Diagnóstico de TI[8] realizado em 2017, foi levantado que muitos órgãos da PMSP possuem equipes defasadas quanto ao número de integrantes, muitas vezes, tais equipes não conseguem desenvolver projetos dado a grande demanda operacional e resolução de problemas, em um posicionamento apenas reativo e sem nenhum posicionamento estratégico devido à quantidade de servidores não adequada. Dado que as metas e operação dos órgãos setoriais são diretamente dependentes da TIC, as operações e serviços das áreas de TIC devem ser devidamente planejados, especialmente quanto à composição da equipe.

8. Diagnóstico de TI. Disponível em: < https://tecnologia.prefeitura.sp.gov.br/diagnostico2017/ >.

LÍDER DE TIC

O líder de TIC é a pessoa chave para as decisões relacionadas à TIC dentro do órgão setorial e possui algumas responsabilidades, tais como: preenchimento do Diagnóstico anual de Tecnologia da Informação e a elaboração, submissão e monitoramento do Plano Direto Setorial de Tecnologia da Informação e Comunicação.

A preferência por um funcionário de cargo efetivo para tal posição se dá pelo posicionamento estratégico da área TI, como por exemplo, a participação nas decisões do orçamento de TIC e cumprimento do Plano Estratégico de TIC - PETIC, a adaptatividade na gestão do conhecimento das decisões gerenciais, além de ser um elemento de motivação para a carreira em TIC na PMSP.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- As áreas de TIC dos órgãos setoriais da PMSP devem possuir pelo menos uma pessoa responsável pela área. Tal pessoa responderá como líder de TIC do órgão.
- Cada líder de TIC deve ter uma pessoa que possa o substituir no caso de sua ausência. A pessoa que substituir o líder de TIC deve ter o respaldo da equipe e direção do órgão setorial, além de possuir conhecimento da área e seus principais processos.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- No caso de ausência do líder de TIC, o substituto deve ser de preferência de dentro da unidade setorial.

CAPACITAÇÃO

Com o intuito de aperfeiçoar as competências gerenciais e técnicas de pessoal, o PETIC, como instrumento de governança de TIC na PMSP, propõe um programa Permanente

de capacitação em TIC voltado para o desenvolvimento dos servidores que atuam na área de TIC e tem como objetivo principal capacitá-los técnica e profissionalmente para melhoria no desempenho de suas atividades.

Entretanto, visando ao aperfeiçoamento das atividades específicas, cada órgão setorial deve possuir o seu próprio Plano anual de Capacitação, envolvendo os servidores das áreas de TIC para fins do aprimoramento de seus conhecimentos e da evolução da sua atuação.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Elaborar e implantar um Plano Anual de Capacitação que procure desenvolver as competências gerenciais e técnicas necessárias à operacionalização da governança, da gestão e do uso da TIC.
- O Plano Anual de Capacitação deve estar de acordo com as metas e objetivos do órgão setorial e deve ser definido juntamente ao Plano Diretor Setorial de TIC – PDSTIC do próprio órgão. Tal plano deve contemplar capacitações para os líderes e para os servidores da área de TIC.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- O Plano Anual de Capacitação pode incluir a participação em cursos gratuitos ou de baixo custo alinhados às necessidades de TIC.
- O líder de TIC deve promover a participação dos servidores de TI a cursos e eventos, relacionados ou não às necessidades de TI da área, mas que promovam maior qualificação profissional do servidor.
- Os líderes de TIC devem buscar capacitação na área de riscos e tomada de decisões.

DIMENSIONAMENTO DA EQUIPE DE TIC

Parte-se do princípio de que não existe uma fórmula única para o qual seja possível definir um número exato de pessoas para integrar uma equipe de TIC. Quer sejam dados o tamanho, atividades e orçamento do órgão. Entretanto, métricas coletadas globalmente pela Gartner[9] nos mostram números e médias que podem balizar e direcionar a tomada de decisão dos líderes de TIC quanto ao tamanho da equipe.

Apenas a título de referência, o Conselho Nacional de Justiça emitiu a Resolução no 211, com valores de referência para as realidades do Judiciário. Deve-se ressaltar a importância de se considerar as demandas de força de trabalho conforme a realidade de cada Órgão Setorial. Para isso, a capacitação do gestor de TIC do órgão setorial para o adequado dimensionamento da sua força de trabalho é algo bastante desejável.

É relevante considerar servidores do quadro permanente dado que o planejamento estratégico através dos anos e gestões depende da gestão do conhecimento executada por tais servidores.

QUANTIDADE MÍNIMA DE PESSOAL

Uma quantidade mínima de pessoal dedicada a área de TIC foi estipulada para sanar as necessidades básicas dos órgãos setoriais. Deve-se pensar nas necessidades de cobrir a ausência de funcionários em situações ocasionais, emergenciais e manter a prestação de serviços de TIC ativa.

9. IT Key Metrics Data 2018: Key industry Measures: Government - State and Local Analysis: Current Year.

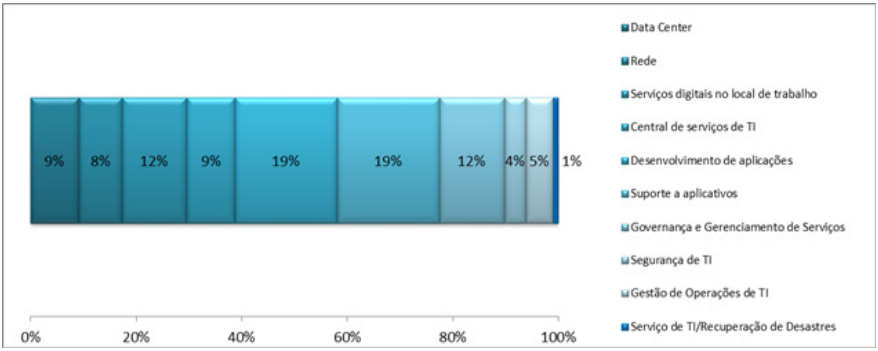
QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Para um órgão setorial que possua acima de 100 usuários de serviços de TIC, dever haver no mínimo quatro servidores dedicados aos assuntos de TIC, desses quatro servidores, no máximo dois podem ser estagiários.
- Um órgão setorial que possua acima de 1000 usuários de serviços de TIC deve possuir uma divisão funcional na área de TIC.
- A quantidade de pessoas dedicadas à TIC em um órgão setorial deve ser planejada segundo a demanda de trabalho e/ou a divisão funcional da área de TIC.
- Investir em capacitação do gestor de TIC do órgão setorial para melhor dimensionamento da demanda de trabalho e da força de trabalho.

PLANEJAMENTO DA NECESSIDADE DE PESSOAL

As pesquisas e análise de dados históricos colaboram para se prever a quantidade de pessoas para uma unidade de TI, além do conhecimento e análise do tamanho, atividades e orçamento do órgão se fazem fundamental, o estilo de gestão e o posicionamento do líder do setor de TIC.

Abaixo, segue uma tabela (referência Gartner) com distribuição de pessoal por função técnica, a qual fornece uma visão consumo dos principais recursos de TIC no contexto do portfólio geral



Área Funcional	Distribuição de recursos
Data Center	9%
Rede	8%
Serviços digitais no local de trabalho	12%
Central de serviços de TI	9%
Desenvolvimento de aplicações	19%
Suporte a aplicativos	19%
Governança e Gerenciamento de Serviços	12%
Segurança de TI	4%
Gestão de Operações de TI	5%
Serviço de TI/Recuperação de Desastres	1%

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Estabelecer um programa de medição de desempenho de TIC para identificar com mais assertividade a alocação de recursos. IT Key Metrics Data 2022: Key industry Measures: Government - State and Local Analysis: Current Year

QUAIS SÃO AS NOSSAS SUGESTÕES?

- A área de TIC de cada órgão setorial da PMSP deve fazer um estudo e análise da quantidade de pessoas alocadas nos serviços de TI, tal estudo permitirá um melhor entendimento e servirá de suporte para tomada de decisões, tais como diminuição ou aumento do quadro de funcionários, buscando assim uma maior eficiência e produtividade da área.
- Analisar a demanda de serviços de TIC do órgão setorial.
- Observar quais as tendências atuais por função técnica para auxiliar no alinhamento com o negócio e na avaliação de metas.

ANALISANDO A DEMANDA

DE TRABALHO E NECESSIDADES

A definição da quantidade de integrantes para equipe levará em consideração vários fatores, dentre eles, a experiência do líder de TIC frente às atividades e a um levantamento e estudo da demanda de trabalho e necessidades da área e do órgão setorial.

A análise da demanda certamente pode ser auxiliada por ferramentas de gestão ou sistemas ITSM (Information Tecnology Service Management) - Sistema de gestão de serviços de TIC. As definições dos processos de trabalho, organização da equipe e hierarquia também colaboram para a análise da demanda do setor.

Elencou-se quatro das principais atividades para análise da demanda de trabalho nas áreas de TIC, as quais são apresentadas na figura abaixo:

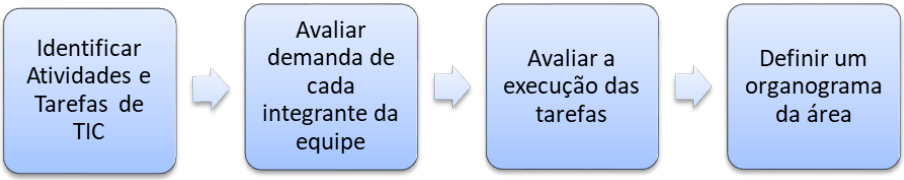


Figura 4 – Análise de demanda de trabalho das áreas de TIC.

IDENTIFICAR AS ATIVIDADES E TAREFAS DESEMPENHADAS PELO SETOR DE TIC

Devem-se listar todas as tarefas e atividades que a área de TIC executa, assim como as responsabilidades que possui perante a gestão do órgão setorial a qual pertencem e ao órgão central de TIC da PMSP.

Um catálogo de serviços pode colaborar na identificação dessas atividades., além de ferramentas e frameworks que

também podem ser utilizados. É importante lembrar que embora algumas das atividades possam não estar sendo desenvolvidas, por quaisquer motivos, elas ainda são atribuições do setor e também devem ser identificadas.

Juntamente com a identificação da ação, se possível, faça uma estimativa do tempo gasto para execução de tal tarefa ou atividade, esse dado possui relevância para o registro de demandas da área.

AVALIAR A DEMANDA ATUAL DE CADA INTEGRANTE DA EQUIPE

Liste todos os servidores de sua equipe e associe a cada um as tarefas e atividades que desenvolve, podendo haver repetição e compartilhamento de tarefas entre os integrantes. Esta é uma análise fundamental para verificar se as tarefas que estão sendo executadas cumprem toda a demanda de seu setor, se os colaboradores estão sendo sobrecarregados ou há falta de pessoal na equipe.

A definição de job descriptions ou descrição do trabalho pode ajudar o gestor a entender melhor o papel e atribuição de cada servidor da área de TIC. Uma breve conversa com os servidores poderá ajudar na descrição dos cargos da área de TIC do órgão e na percepção se a demanda de trabalho está adequada para a quantidade de pessoas atuantes na área de TIC de seu órgão.

Uma descrição do trabalho também pode colaborar para contratação de novos profissionais pois tem elencadas em um documento formal as competências necessárias para a posição em questão, o tipo de profissional esperado e a síntese das atividades a serem executadas.

Dado o tamanho da atuação do órgão setorial, este passo pode ser feito em abordagem top-down, avalia-se a demanda das equipes ou grupos funcionais como um todo e não individualmente dos integrantes.

AVALIAR A EXECUÇÃO DAS TAREFAS

Verificar se as tarefas estão sendo executadas adequadamente e se estão sendo atribuídas aos servidores de acordo com o seu perfil profissional e qualificação técnica. Perguntas como as apresentadas a seguir contribuirão para identificar se a quantidade de pessoas na equipe está satisfazendo as necessidades da área:

- **Os serviços e tarefas demandados são corretamente realizados?**
- **A equipe possui as competências exigidas para pleno funcionamento da área?**
- **A quantidade de pessoas é suficiente para atender à demanda?**
- **O líder se concentra nas atividades de gestão do setor?**

DEFINIR UM ORGANOGRAMA DA ÁREA

É necessário entender quais os cargos que compõem a área de TIC para avaliar a demanda de trabalho da equipe. Devem-se mapear todas as posições e hierarquias, mesmo que não estejam ocupadas, anotando a quantidade de funcionários e cargos, esse mapeamento permitirá uma fácil visualização e compartilhamento da atual situação do quadro de servidores trabalhando na área de TIC.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Coletar informações utilizando-se de atividades de análise da demanda e apresenta-las de maneira organizada para os tomadores de decisão pedindo adequação da quantidade de colaboradores de acordo com suas especificações técnicas para uma melhor execução do serviço prestado pela TIC.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Criar um catálogo de serviços para a área de TIC do órgão setorial.
- Utilizar um SGSTI para a gestão de serviços área de TIC do órgão setorial.
- Utilizar a divisão funcional apresentada no próximo capitulo para definir o organograma da área.

NÍVEIS DE ATUAÇÃO

Dentro das áreas de TIC existem servidores que enxergam longe e apresentam pensamento crítico em relação aos serviços do órgão e seu futuro, assim como também existem aqueles com mais facilidade para planejar e executar os processos internos da organização. São perfis diferentes, mas que se complementam para garantir que os objetivos do Órgão Setorial sejam alcançados.

Visando uma melhor identificação do papel dos servidores das áreas de TIC dos órgãos setoriais da PMSP, a atuação dos servidores pode ser classificada em três níveis básicos: **Estratégico, Tático e Operacional**.

Figura 5: Níveis Estratégico, Tático e Operacional

Um servidor de nível mais alto na pirâmide poderá possuir tarefas e atuar como os níveis abaixo dele, porém sempre será classificado como o nível mais alto.

NÍVEL ESTRATÉGICO

O líder de TIC por padrão atua no nível estratégico da área de TIC e é responsável pelo planejamento e direcionamento de todo o trabalho desenvolvido na área de TIC.

O profissional alocado no perfil estratégico deve ter uma visão crítica da área: saber avaliar as necessidades, identificar riscos, antecipar tendências e planejar o futuro. São pessoas que pensam além das tarefas rotineiras e que apresentam bons insights sobre qual deve ser o direcionamento da área de TIC e quais são as principais ações que devem ser planejadas para a evolução contínua da área.

Servidores de TIC com perfil estratégico têm uma visão geral do órgão, incluindo o conhecimento da sua história e cultura; capacidade para analisar os dados, sempre pensando no crescimento da maturidade; atenção para enxergar novas oportunidades de melhoria e iniciativa para experimentar novos processos e ferramentas. O alinhamento do líder de TIC com a direção e gabinete do órgão ao qual faz parte também possui relevante importância para o alinhamento entre a TIC e os processos de negócio.

As contribuições do profissional de perfil estratégico como líder de área são essenciais para a transformação digital do órgão a qual está inserido, além de ser contato para execução do Plano Estratégico de TIC estabelecido para o Município.

NÍVEL TÁTICO

Este servidor apresenta uma visão específica de alguma função da área de TIC ou do Órgão em que atua. Dividir objetivos em projetos e/ou atividades que podem ser delegadas e detalhadas é algo que faz parte da sua rotina de trabalho e, por

conta disso, não raro atua como gestor de outros servidores e terceiros contratados.

O profissional do nível tático é o responsável por traduzir os objetivos, estabelecidos pelo servidor de nível estratégico, em iniciativas para materializá-los. Ao mesmo tempo, tem a capacidade de identificar as necessidades do nível operacional e propor e/ou implementar soluções, levando propostas para o nível estratégico, caso necessário. Ele consegue enxergar quais são as responsabilidades do seu setor para que as metas propostas sejam atingidas e tem capacidade de organização para planejar ações práticas.

- **NÍVEL OPERACIONAL**

Servidores do perfil operacional atuam de forma técnica, resolvendo incidentes, problemas e trabalhando para a concretização de projetos. Possuem capacidade para definir métodos e processos para alcançar, em um prazo adequado, os objetivos da área e estão aptos para entregar resultados para as ações planejadas.

O profissional operacional também é capaz de se organizar para cumprir cronogramas, com capacidade adequada para executar os projetos e/ou as atividades do dia-a-dia, contribuindo para que as iniciativas da área sejam bem executadas e dentro do prazo planejado.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Identificar os servidores que trabalham na área de TIC de acordo com os 3 níveis de atuação apresentados, realizando a capacitação e a atribuição das atividades conforme cada perfil.
- No caso da área de TIC possuir servidor que atue rotineiramente nos três níveis, tomar ações para que tal servidor passe a atuar no máximo em dois níveis.

DIVISÃO FUNCIONAL

Cada uma das áreas de TIC dos órgãos da PMSP trabalha de uma maneira diferente e inúmeros são os tipos de serviços prestados, pois podem ser resultantes das atividades e metas dos órgãos em questão. Consequente, devido a diversidade de realidades, não existe uma estrutura de divisão funcional que possa ser utilizada como padrão para as áreas de TIC da PMSP. Entretanto, é possível identificar grupos de atividades que são comuns de maneira a categorizá-las em funções, utilizando para isso um modelo organizacional.

Tais funções são independentes do número de integrantes da equipe, podendo ser exercidas por uma ou mais pessoas, podendo os servidores executar atividades de uma ou mais funções, o modelo não é rígido, pode-se adicionar funções à medida que as responsabilidades e expectativas se transformam.

A seguir apresentamos um modelo adaptado para a realidade da PMSP baseado em modelo funcional apresentado pelo Gartner[3] de uma organização de TIC para governo, descrito a um nível organizacional, tal modelo pode ser utilizado como base para a descrição das funções dos setores de TIC.

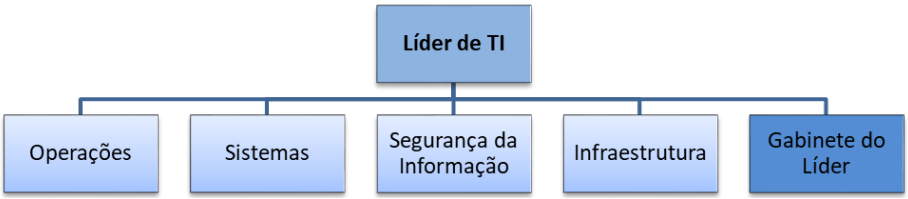


Figura 6 - Divisão funcional da área de TIC.

LÍDER DE TIC — É o responsável por toda a área de TIC do orgão setorial da PMSP e por implementar a Política de Governança do Decreto 57. 653 de 07 de Abril de 2017 . No modelo desempenha o mesmo papel de um CIO em uma estrutura empresarial.

OPERAÇÕES — Responsável pelas operações de TI, a função de operações inclui gestão de portais, usuários, rede interna, links de conectividade e o help desk/suporte ao usuário. Em particular, o suporte de usuário inclui questões sobre desempenho, abordando os requisitos de capacidade e geração de relatórios, por exemplo.

SISTEMAS — Lida tanto quanto com a aquisição e/ou customização de sistemas disponíveis no mercado, tais como ERP e CRM, bem como o desenvolvimento de sistemas específicos. Exige capacidades para ajudar no desenvolvimento de aplicações sob medida entre os padrões e processos de desenvolvimento estabelecidos pela organização de políticas.

SEGURANÇA DA INFORMAÇÃO — Cuida do desenho, implementação e gestão dos projetos relativos à segurança da informação em termos de tecnologia da informação e comunicação. É importante ressaltar que essa função deve conversar com todas as outras, pois a segurança deve permear todas as atividades de tecnologia da informação e comunicação.

INFRAESTRUTURA — Responsável por projetar e gerir iniciativas relativas a processos envolvendo Capacidade, Disponibilidade e Continuidade de Serviços, além de gerir o Data Center e estruturas complexas similares de infraestrutura.

GABINETE DO LÍDER — O gabinete cuida de iniciativas de cunho estratégico, como o planejamento estratégico e iniciativas voltadas para a transformação digital. Além disso, o gabinete trata também de questões táticas, como o

Escritório de Projetos (PMO – Project Management Office), que realiza a supervisão do portfolio de projetos da área de TI, além de executar tarefas operacionais subsidiárias, como a gestão de contratos que não sejam diretamente afeitos a nenhuma das outras funções (ex: contratos de capacitação), além de estabelecer padrões e processos para as atividades das outras áreas.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Verificar se a área de TIC do órgão setorial possui ações nas funções descritas no modelo apresentado, identificar e definir os serviços da área de TIC dentro da divisão apresentada.
- Identificar o responsável ou responsáveis pelas atividades de cada função.
- Adaptar o modelo da divisão funcional proposto à realidade do seu órgão e à área de TIC.
- Órgãos setoriais que contam com mais de 1000 usuários de serviços de TIC deverão possuir equipes e consequentemente líderes para as divisões funcionais conforme demandas das áreas.

QUANDO AS RECOMENDAÇÕES PASSAM A VALER?

Os procedimentos descritos nesta Orientação Técnica deverão ser aplicados nos procedimentos atuais e futuros, bem como nos contratos futuros e nas prorrogações contratuais, ainda que de contratos assinados antes do início da vigência desta OT.

Esta Orientação Técnica entrará em vigor a partir da sua aprovação pelo CMTIC.

REFERÊNCIAS

Link: http://www.cnj.jus.br/atos-normativos?documento=2227 - Conselho Nacional de Justiça. Resolução Nº 211 de 15 de Dezembro de 2015. Acessado em: 03/03/2023.

Guia: Gartner, Inc. How to Establish a Service-Optimized Organizational Structure, 2016.

Guia: Gartner, Inc. IT Key Metrics Data 2022: Key industry Measures: Government - State and Local Analysis: Current Year.

Guia: Gartner, Inc. IT Organizational Design CIO Desk Reference Chapter 28, 2018

Link: https://tecnologia.prefeitura.sp.gov.br/diagnostico2017/ - Prefeitura de São Paulo. Gov.IT - Portal de Governança de TIC. Diagnóstico de TIC, 2017.

Link: https://tecnologia.prefeitura.sp.gov.br/?page_id=3366 - Prefeitura de São Paulo. Gov.IT - Portal de Governança de TIC. Plano Estratégico de Tecnologia da Informação e Comunicação

Em caso de dúvidas, o Portal de Governança de TI (http://forum.govit.prefeitura.sp.gov.br/) é o local principal em que elas poderão ser expostas, discutidas e solucionadas, de forma a fomentar o aumento e melhoria de conhecimentos e procedimentos, bem como a sua disseminação.

Além do Portal, O Órgão Central do Sistema Municipal de Tecnologia da Informação e Comunicação está à disposição para dirimir eventuais dúvidas advindas desta Orientação.

Órgão Central - Coordenadoria Geral de Tecnologia da Informação e Comunicação (CGTIC): http://tecnologia.prefeitura.sp.gov.br

OUTRAS ORIENTAÇÕES TÉCNICAS

VOL.1

[OT 001] Aquisição de bens de microinformática

[OT 002] Interconectividade de redes

[OT 003] Serviços de impressão e digitalização

[OT 004] inventários de ativos e licenças de software

[OT 005] padrões de rede interna

VOL.2

[OT 006] Links de conectividade internet

[OT 007] Backup e armazenamento de dados

[OT 008] Acessibilidades digitais na administração municipal

[OT 009] Aquisições de serviços de computação em nuvem

[OT 010] Critérios gerais de gestão de aplicações

VOL.3

[OT 011] Diretrizes para contratos de sustentação de TIC e similares

[OT 012] Modelos de contratação e métricas de dimensionamento de sistemas

[OT 013] Diretrizes básicas de segurança da informação

[OT 014] Adequações do espaço físico de trabalho de TIC

[OT 015] Adequação da equipe de TIC

VOL.4

[OT 016] Licenças de software e código aberto

[OT 017] Gestão dos bens inservíveis de tic