ORIENTAÇÕES TÉCNICAS
GERAIS DE TIC

VOL.2

[OT 006-010]

CGTIC

CIDADE DE SÃO PAULO
INOVAÇÃO E TECNOLOGIA

ORIENTAÇÕES TÉCNICAS

GERAIS DE TIC

VOL.2

[OT 006-010]

CGTIC

CIDADE DE SÃO PAULO
INOVAÇÃO E TECNOLOGIA

Coordenadoria de Gestão de Tecnologia da Informação e Comunicação
E-mail: tecnologia@prefeitura.sp.gov.br
Endereço: Rua Líbero Badaró, 425 — 27º andar — Centro
Telefones: 55 11 2392-2092 | 55 11 2075-7240

SUMÁRIO

06
APRESENTAÇÃO

07
INTRODUÇÃO

08
DEFINIÇÕES GERAIS

09
LINKS DE CONECTIVIDADE DE INTERNET [OT 006]

30
BACKUP E ARMAZENAMENTO DE DADOS [OT 007]

47
ACESSIBILIDADE DIGITAL NA ADM. MUNICIPAL [OT 008]

62
AQUISIÇÕES DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM [OT 009]

97
CRITÉRIOS GERAIS DE GESTÃO DE APLICAÇÕES [OT 010]

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-006/OT-010) 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 006]
LINKS DE CONECTIVIDADE DE INTERNET

10 ESCOPO E CONTEXTO

10 CRITÉRIOS GERAIS

12 TECNOLOGIAS FÍSICAS DE ACESSO

24 DIMENSIONAMENTO

Busca orientar a respeito de tecnologias físicas de acesso como fibra óptica, cabeamento metálico e cabeamento sem fio, bem como o dimensionamento de links de internet adequado a quantidade de usuários e aplicações e a estimativa de banda a partir de perfis de usuários.

ESCOPO E CONTEXTO

Fazem parte do escopo desse documento as diretrizes a respeito dos parâmetros a serem considerados para a estimativa de largura de banda e a escolha técnica das tecnologias para links de conectividade à internet.

Os Órgãos Setoriais poderão adotar diferentes modelos de contratação, avaliando possibilidades como a contratação de um managed services provider (MSP) que forneça inclusive os ativos de rede (roteadores e demais materiais) para o acesso físico à conexão mais adequada, bem como o modelo mais adequado de contratação, em aderência com os requisitos de negócio e a viabilidade técnica-orçamentária.

Não fazem parte do escopo desta OT as medidas de segurança e de segregação de infraestrutura para a conexão à internet, tampouco as questões de caráter operacional da instalação, configuração ou operação da conexão.

CRITÉRIOS GERAIS

Dentre os parâmetros técnicos a serem considerados na contratação de um serviço de internet, os mais objetivos são:

Largura de Banda: é a taxa de transmissão de dados usualmente especificada em bits por segundo (bps) ou seus multiplicadores mais usuais: Kbps, Mbps ou Gbps.

Throughput: é a capacidade efetiva de transmissão de um canal ou sistema, e utiliza as mesmas unidades da largura de banda;

IP fixo ou dinâmico: um fornecedor pode fornecer um ou mais IPs fixos ou ainda ter um IP dinâmico, isto é, um IP que é trocado periodicamente. Uma conexão com IP dinâmico tem custo mais acessível, via de regra. Um link de internet sempre terá pelo menos um IP público de internet.

Confiabilidade: é a recorrência da perda de pacotes na transmissão.

Latência e Jitter: latência em comunicação de dados é o tempo que um evento demora para ocorrer a partir de seu acionamento, como por exemplo a confirmação do recebimento de um pacote vindo da ponta remota. Jitter é a variação da latência. No caso de VoIP, desencadeia má qualidadade da voz. O uso de buffers de jitter foi concebido para acabar com tal problema, mas requer um limite de cerca de 20 milissegundos de variações de atraso;

Disponibilidade e Redundância: A disponibilidade é o índice que mede a estabilidade de um sistema. Ele é obtido a partir do tempo de indisponibilidade de um sistema, em relação ao tempo total do período considerado. A redundância refere-se a posse de componentes de reserva, instalados e prontos para atuarem como substitutos dos componentes primários, no caso de estes falharem.

Escalabilidade: O dimensionamento adequado da banda de conectividade é fundamental para que a conexão alcance os seus objetivos de negócio. Esse dimensionamento contempla não apenas as necessidades imediatas, mas também as estimativas de demandas futuras, para mitigar a queda na qualidade dos processos de negócio em caso de crescimento da demanda.

Em termos técnicos, valem também as seguintes considerações adicionais:

- Embora alguma latência seja tolerável, e até prevista, ela é um fator crítico para aplicações que funcionam em tempo real, tais como chamadas de voz e vídeo, por exemplo, onde valores de latência superiores a cerca de 150 milissegundos impactam negativamente no uso das aplicações. Um roteador com a função QoS (Quality of Service) permite priorizar pacotes e mitigar este problema.

- É importante perceber que uma disponibilidade contratual de 99,9 % traduz 8 horas e 46 minutos indisponíveis no período de um ano. Já uma disponibilidade de 99,99% representa 50 minutos de indisponibilidade em um ano.
- Sempre que houver impacto ao serviço prestado pela falta de conectividade, é preciso pensar a contratação de redundância, isto é, um segundo link (ou VPN) com infraestrutura diferente do principal que atenda minimamente às operações.
- Se existir um servidor na infraestrutura interna que necessite ser acessível externamente, há a necessidade de que a contratação preveja no mínimo um IP fixo.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Adotar SLA (Acordo de Nível de Serviço) compatível com a qualidade da conectividade almejada, definindo patamares a serem entregues pelo fornecedor em função dos critérios elencados, do seu uso pelo Órgão Setorial e da disponibilidade orçamentária-financeira, sem prejuízo de demais SLAs para atendimento a outros requisitos, tais como prazos de instalação e de recuperação de serviço.
- Para comunicações em tempo real, adotar patamares máximos de latência e/ou jitter no SLA, de forma a obter comunicação aceitável.
- Avaliar a contratação de um link de redundância, isto é, um segundo link (ou VPN) com infraestrutura diferente do principal que atenda minimamente as operações, no caso em que a falta de conectividade causar impacto técnico relevante aos processos de negócio do Órgão Setorial.
- Prever no mínimo um IP fixo se existir um servidor na infraestrutura interna que necessite ser acessível externamente.
- Avaliar a contratação de conectividade internet com largura de banda assegurada.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Contratar serviços de conectividade internet sem limite (franquia) de volume de tráfego, caso exista tal opção.
- Avaliar o uso de outras métricas para a qualidade da conexão à internet, tais como tempo médio de recuperação de serviço e tempo médio entre falhas.
- Buscar não apenas uma banda maior, mas também latência menor, com a análise da adequação da infraestrutura interna de rede com relação à demanda de consumo.
- Utilizar softwares específicos de medição para avaliar a qualidade de uma conexão, com indicadores tais como latência, perda de pacotes, largura de banda, disponibilidade e jitter, que nem sempre têm informações comerciais disponíveis explícitas entregues pelos fornecedores.
- Investir na capacitação dos servidores de TIC do Órgão Setorial para aprimorar e atualizar os seus conhecimentos sobre as diversas possibilidades e tecnologias de conectividade à internet.

TECNOLOGIAS FÍSICAS DE ACESSO

Cada meio físico de acesso tem sua aplicação, suas vantagens e restrições, que variam conforme a localidade a ser atendida.

O Órgão Setorial tem autonomia para decidir sobre a melhor tecnologia de acesso, de forma a atender as suas necessidades, disponibilidades e peculiaridades, especialmente com relação à sua localização geográfica.

As tabelas a seguir elencam algumas das tecnologias e suas principais características.

FIBRA ÓPTICA

Para transmissão de dados em altas velocidades, a fibra óptica é a tecnologia padrão utilizada atualmente. As tabelas abaixo apresentam de forma bastante resumida os principais tipos e tecnologias de fibra óptica utilizados atualmente.

DESCRIÇÃO	TIPOS	CARACTERÍSTICAS
Fios de fibra de vidro que levam luz, tornando a comunicação imune à intereferência	- Monomodo (para uso geral) - Multimodo (para distâncias menores, como por exemplo redes locais)	- Indicado como tecnologia padrão para backbones (cabeamento vertical) de Órgãos Setoriais. - Indicado como tecnologia padrão para conexões entre o Órgão Setorial e sites externos. - Maior largura de banda e confiabilidade em relação aos demais. - Alto custo, não tanto pela fibra em si, mas pelos equipamentos que, por exemplo, convertem o sinal de luz em sinal elétrico e vice-versa. - Eventualmente, fornecedores não entregam um serviço full-duplex, por uma opção estratégica comercial do fornecedor.

Tabela 1: Descrição simples das características das redes de fibra óptica.

Nome	Tipo	Fast Ethernet 100BASEFX	1 Gigabit Ethernet 1000BASE-SX	1 Gigabit Ethernet 1000BASE-LX	10 Gigabit Ethernet 10GBASE	40 Gigabit Ethernet 40GBASE	100 Gigabit Ethernet 100GBASE
FDDI	Multimodo	2.000m	220m	550m[1]	26m	Não suportado	Não suportado
OM1			275m		33m	Não suportado	Não suportado
OM2			550m		82m	Não suportado	Não suportado
OM3 (otimizado para laser)				550m	300m	100m	100m
OM4 (otimizado para laser)					400m	150m	150m
Monomodo	Monomodo		5.000m@ 1310nm	5.000m@ 1310nm			

Tabela 2: Quadro resumido correlacionando os tipos de fibra óptica às velocidades e comprimentos máximos.

1. Exige patch cable de condicionamento de modo.

TECNOLOGIA	DOWN	UP	CARACTERÍSTICAS	PRINCIPAIS USOS
GPON (ITU-T G.984)	2,488 Gbps	1,244 Gbps	- Suporte nativo ao protocolo ATM, fornece encapsulamento genérico para transmissão Ethernet, IP, TCP, UDP, T1/E1, video, VoIP e outros. - Fornece criptografia AES (apenas para downstream). - Permite a coexistência XGPON e GPON dentro da mesma fibra, por usar comprimentos diferentes de onda.	- Atendimento a maior número de usuários. - Necessidade de oferecer grande gama de serviços, incluindo servidos diferenciados como IPTV, vídeoconferência, vigilância por vídeo IP, e aplicações de nuvem fornecendo serviço online sob demanda para clientes thin. - Demanda por SLAs (Acordos de Nível de Serviço) mais rigorosos. - Exigências de controle e de QoS (Quality of Service – Qualidade de Serviço) mais sofisticados. - Mais comuns no continente americano e europeu.
XGPON ou 10GPON (ITU-T G.987)	10 Gbps	2,5 Gbps		

EPON/GEPON (Ethernet 802.3ah)	1,25 Gbits/s	1,25 Gbps	- Suporte nativo a Ethernet e IP. - Maior facilidade de instalação e configuração. - Controles mais simplificados.	- Atendimento a aplicações de nicho, como por exemplo, em prédios e centros empresariais. - Menor demanda por serviços ou menor maturidade para gerir comunicações via fibra óptica. - Mais comum na Ásia.
10Gbit EPON (Ethernet 802.3av)	10 Gbps	10 Gbps ou 1 Gbps		
TWDM-GPON (implementação do NG-PON2)	10 Gbps ou 2,5 Gbps por canal, máx 40 Gbps	10 Gbps ou 2,5 Gbps por canal, máx 40 Gbps	- Compatibilidade reversa com as tecnologias anteriores de GPON. - Maior convergência de infraestrutura de comunicação. - Facilidade em adequar e balancear as bandas dos canais para atender às necessidades de tráfego.	- Igual aos usos para GPON, mas que exijam maiores capacidades de banda e gerenciamento. - É uma tecnologia emergente.

Tabela 3: Tabela condensada com as tecnologias de conexão utilizando fibra óptica.

No caso particular das fibras ópticas, é necessário avaliar também a forma de transmissão do sinal e o local da sua terminação. A forma de transmissão pode ser ativa ou passiva. A tabela abaixo compara as duas formas.

FORMA DE TRANSMISSÃO	DESCRIÇÃO	VANTAGENS E DESVANTAGENS	ALCANCE
AON (active optical network)	Uso de fibra e de componentes ativos, como amplificadores, repetidores e circuitos de modelagem de sinal.	- Maior alcance - Menor economicidade	100km
PON (passive optical network)	Uso apenas da fibra e componentes passivos na rede, como splitters (divisores) e combinadores	- Maior economicidade - Menor alcance	20km

Tabela 4: Comparativo das formas de transmissão de fibra óptica.

O local de sua terminação influencia em termos de custo e banda/latência, conforme a tabela abaixo.

Local de Terminação	Custo	Banda	Latência
Mais perto do Órgão Setorial	Maior	Maior	Menor
Mais longe do Órgão Setorial	Menor	Menor	Maior

Tabela 5: Comparativo dos efeitos do custo e banda de acordo com o local de terminação.

Existem diferentes possibilidades para o local de terminação. Para fins desta Orientação Técnica, são definidos três grandes tipos:

- Fiber to the Node (ou Fiber to the Neighborhood): a terminação da fibra é feita em um local distante acima de 300 metros do Órgão Setorial;

- Fiber to the Curb: a terminação da fibra é feita em um local distante abaixo de 300 metros do Órgão Setorial;

- Fiber to the Building (ou Fiber to the Premises): a terminação da fibra é feita dentro do Órgão Setorial.

A figura a seguir ilustra as possibilidades citadas acima.

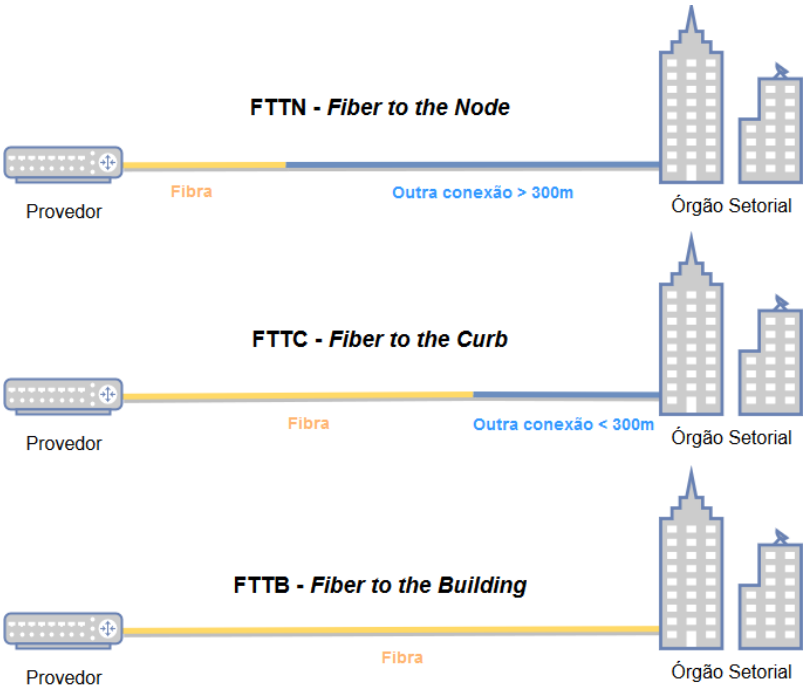


Figura 1: Diferentes locais de terminação da fibra óptica na conexão entre provedor e Órgão Setorial. entre provedor e Órgão Setorial.

CABEAMENTO METÁLICO

O uso de cabeamento metálico é a forma mais tradicional de se ter uma conexão. A tabela abaixo apresenta de forma bastante resumida os principais tipos de tecnologias para cabeamento metálico.

TIPO DA TECNOLOGIA	DESCRIÇÃO	CARACTERÍSTICAS
xDSL (Digital Subscriber Line[2])	Tecnologia que permite a utilização de uma linha telefônica para transmissão de dados. Algumas velocidades típicas: - ADSL: 256 kbps a 8 Mbps - ADSL2/ADSL2+: 256 kbps a 24 Mbps - VDSL: até 52 Mbps - VDSL2: até 100 Mbps	- Exige a contratação de um provedor de acesso web, além da concessionária telefônica. - Realiza o compartilhamento da infra-estrutura, de forma que a velocidade é inversamente proporcional à quantidade de usuários. Desta forma, as concessionárias deixam claro no contrato de serviço que garantem apenas uma parcela (geralmente 10%) da velocidade nominal contratada. - A velocidade cai conforme aumenta a distância à central telefônica. - Para a categoria ADSL, o upload é menor que o download por uma restrição da tecnologia.
Cable Modem (padrão DOCSIS 2.x ou 3.x)	Tecnologia que usa o mesmo canal usado para transmitir o sinal de TV a cabo, utilizando um splitter para separar o sinal da TV dos dados da rede e um cable modem para acessar a rede. Velocidade típica: 1 Mbps a 150 Mbps	- De forma geral, a velocidade de upload é menor que a de download. - A oferta deste tipo de acesso está restrita às regiões onde também existe o serviço de TV paga via cabo. - Vantagem de ter uma conexão com a web permanentemente ativa, bastando ligar o computador. - A velocidade da conexão varia menos do que os outros tipos de cabeamento metálico. - A provedora de serviço pode oferecer planos com franquia (limite) de dados.

2. As duas categorias mais comuns são o ADSL (Asymmetric DSL) e o SDSL (Symmetric DSL), sendo que o primeiro costuma predominar sobre o segundo no Brasil. Outras possibilidades podem ser, por exemplo, HDSL (High data rate DSL) e VDSL (Very high DSL).

EoC (Ethernet over Copper)	Assim como o xDSL, é uma tecnologia que permite a utilização de uma linha telefônica para transmissão de dados. Necessita de equipamento específico. Velocidade típica: 2 Mbps a 45 Mbps	- Via de regra, possui melhor desempenho do que xDSL, tanto em termos de banda quanto em termos de latência e confiabilidade. - Assim como o xDSL, a velocidade cai conforme aumenta a distância à central telefônica. Entretanto, a queda de velocidade costuma ser mais acentuada do que redes xDSL, exigindo maior proximidade geográfica com a central.
E1/E1 fracionário[3]	Serviço de linha alugada, usado para comunicação banda larga. Velocidades típicas: - E1: 1,920 Mbps - E1 fracionário: velocidades inferiores a E1.	- A velocidade da conexão varia menos do que os outros tipos de cabeamento metálico.
Internet pela rede elétrica/PLC (Power Line	Serviço que utiliza as linhas de transmissão de energia para transmissão de dados para a rede. Velocidade teórica esperada: - Até 40 Mbps	- Ainda em fase experimental, apesar da sua oferta já ter sido regulamentada pela Anatel. - Facilidade de implantação, por utilizar uma infraestrutura já existente. - Velocidade síncrona (o upload tem a mesma banda do download).

Tabela 6: Quadro simplificado descrevendo algumas tecnologias para cabeamento metálico.

3. A tecnologia E1 é adotada como padrão no Brasil e na Europa. Nos EUA, a tecnologia equivalente é T1/ bonded T1/T3, com velocidades que variam de 1,544 Mbps (T1) a 44,736 Mbps (T3).

COMUNICAÇÃO SEM FIO (WIRELESS)

A tabela abaixo apresenta de forma bastante resumida os principais tipos de tecnologias para comunicação sem fio.

TIPO	DESCRIÇÃO	CARACTERÍSTICAS
Rádio	Ondas de rádio são um tipo de radiação eletromagnética transmitidas pelas torres distribuídas em pontos altos e com bom acesso ao perímetro atendido pelo provedor. Para receber a internet, uma antena é instalada no domicílio do usuário e fica responsável por captar do sinal emitido por uma das torres.	Não utiliza linha telefônica; Baixo custo de manutenção; Obstáculos entre a torre e a antena prejudicam a conexão; Problemas de estabilidade em caso de mau tempo; Frequências entre 2,4 GHz até 66 GHz;e Baixa taxa de transmissão.
Microondas	São ondas eletromagnéticas com comprimentos maiores que os dos raios infravermelhos, mas menores que o comprimento das onda de rádio. Suas frequências situam-se entre 2,0 a 40 Ghz. Em redes de computadores, geralmente operam entre 2,4Ghz e 5 Ghz. Taxa de transmissão de até 600 Mbps (2,4Ghz) e 300 Mbps (5Ghz).	É possível fazer a ligação entre duas redes usando ligação ponto a ponto sem fio, usando-se de duas antenas direcionais, uma em cada rede. As antenas precisam estar perfeitamente alinhadas e portanto, só funciona para comunicação em linha reta, sem obstáculos. O alcance máximo vai depender das antenas utilizadas.

Satélite	As ondas de satélite são utilizadas em comunicações intercontinentais ou abrangendo grandes distâncias geográficas, estando sujeitas a atrasos devido às grandes distâncias percorridas. Taxa de transmissão entre 5 e 22 Mbps.	Acesso independente de localização, disponível mesmo nos pontos mais remotos, com boa disponibilidade. Custo elevado. Latência grande (acima de 200ms), principalmente pela distância até o satélite.
Infravermelho	Os raios infravermelhos podem ser utilizados para transmitir sinais digitais entre computadores (assim como é utilizado em televisões, vídeos, automóveis, etc). Para tal, torna-se necessário que estes se encontrem relativamente próximos uns dos outros, além de não haver barreiras físicas entre os dispositivos. Taxa de transmissão de até 10 Mbps.	São mais susceptíveis a inteferências por luz solar e fontes de calor; São simples e baratas, além de não necessidar de licenças governamentais.

Tabela 7: Quadro simplificado descrevendo algumas tecnologias para comunicação sem fio (wireless).

Analisando-se as características das diferentes tecnologias de conexão, é possível constatar que a fibra óptica é a que fornece os maiores benefícios e capacidades para uma conexão com alta disponibilidade de banda e baixa latência.

Da mesma forma, a conexão via cable modem e a conexão via microondas são as melhores opções técnicas para ter maior disponibilidade de banda na comunicação via cabeamento metálico e sem fio, respectivamente.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Verificar as especificações dos ativos de rede a serem usados na conexão, para confirmar a sua adequação ao uso, notadamente as especificações relativas à velocidade e à distância no caso de envolver comunicação utilizando fibra óptica.
- Buscar a conexão utilizando fibra óptica como primeira opção, utilizando-se os demais meios físicos de forma subsidiária, em caso de particularidades técnicas que não indiquem a conexão baseada inteiramente em fibra como sendo a melhor opção.
- Para conexão à internet utilizando fibra óptica, buscar o uso de fibras monomodo em PON (rede passiva) como padrão, por conta da sua economicidade.
- Para conexão à internet utilizando cabeamento metálico, buscar o uso da conexão baseada em cable modem como padrão e as demais tecnologias de forma subsidiária, em caso de particularidades técnicas que não indiquem a conexão via cable modem como melhor opção.
- Para conexão à internet utilizando comunicação sem fio, buscar o uso da conexão baseada em microondas como padrão e as demais tecnologias de forma subsidiária, em caso de particularidades técnicas que não indiquem a conexão via microondas como melhor opção.

- Analisar os parâmetros técnicos dos serviços oferecidos sem se ater ao seu nome fantasia (tais como “dedicado” ou “banda larga”), para verificar se atendem às necessidades do Órgão Setorial.

DIMENSIONAMENTO

Um link deficiente pode aumentar o tempo de resposta, o que diminui a produtividade e aumenta o tempo de resposta aos serviços prestados, ou pode, no pior dos cenários, ser totalmente inadequado para a atividade fim.

O correto dimensionamento de um link de internet passa por considerar a quantidade de usuários e aplicações que rodarão simultaneamente; a criticidade do serviço; e estimar uma banda que atenda esta demanda.

Para a estimativa de banda, esta Orientação Técnica define quatro diferentes perfis de usuário, classificados de acordo com o seu uso de internet:

1. Usuário básico:

- Navegação Web;
- E-mail;

2. Usuário moderado:

- Downloads frequentes;
- Serviços de streaming;
- Serviços baseados em nuvem;
- VOIP;

3. Usuário de multimídia:

- Alto volume de downloads;
- Web Interativa;
- Videoconferência;

4. Usuário avançado:

- Alta demanda de banda, como por exemplo, telemedicina e backup na nuvem;
- Aplicação web de uso intensivo como plataforma de educação à distância;
- Múltiplos dispositivos por usuário;

Para cada perfil, tem-se a banda mínima, a banda razoável e a banda ideal de internet. A tabela a seguir mostra esses dados para o dimensionamento, considerando-se grupos de 10 usuários.

Perfil do Usuário	Banda mínima (Mbps/10 usuários)	Banda ideal (Mbps/10 usuários)
Básico	1	2
Moderado	1	4
Multimídia	2	6
Avançado	3	8

Tabela 8: Dimensionamento da banda por perfil de usuário.

O cálculo é feito da seguinte forma:

1. Levantar o quantitativo de usuários para cada perfil;
2. Dividir cada quantitativo por dez, arredondando para cima em caso de não ser uma divisão errada;
3. Multiplicar os quantitativos pelos respectivos valores da tabela acima;
4. Somar os valores para obter a largura de banda.

Exemplo Hipotético: Determinada Prefeitura Regional fez o seguinte levantamento de perfis para seus usuários:

- Básico: 170 usuários
- Moderado: 19 usuários
- Multimidia: 1 usuário
- Avançado: 0 usuário

Dividindo-se os quantitativos e fazendo-se o arredondamento, tem-se:

- Básico: 17
- Moderado: 2 (1,9 arredondando para cima)
- Multimídia: 1 (0,1 arredondando para cima)
- Avançado: 0

Assim, a banda mínima de internet para essa Prefeitura Regional seria:

$$[17 \times 1] + [2 \times 1] + [1 \times 2] + [0 \times 3] = 21 \text{ Mbps}$$

Da mesma forma, a banda ideal de internet para esse caso seria:

$$[17 \times 2] + [2 \times 4] + [1 \times 6] + [0 \times 8] = 48 \text{ Mbps}$$

Assim, para atender a essa Prefeitura Regional, é adequado contratar um link com o mínimo de 21 Mbps. É interessante buscar a contratação de um link de 48 Mbps mas, acima disso, as melhoras de desempenho não são tão claramente perceptíveis.

A quantidade de usuários e o tipo de aplicação de cada perfil têm reflexo direto na largura de banda a ser contratada. Os perfis apresentados são os básicos e o Órgão Setorial possui autonomia para inserir outros perfis conforme a realidade local.

Além disso, o dimensionamento deve levar em consideração se o Órgão Setorial trabalha com transmissão de dados

em burst. Neste caso, há a necessidade de verificar se o tempo de transporte do volume de dados é adequado para finalidade específica.

Um exemplo ilustrativo: Considerando-se um canal exclusivo ideal de 2Mbps, quanto tempo será necessário para transmitir um arquivo de radiografia de 6 Mbytes para um servidor remoto?

O tempo de transferência se dá pela divisão de 6 Mbytes por 2 Mbps (lembrando-se que 1 byte é o mesmo que 8 bits) e tem-se 6x8/2 = 24 segundos.

Dependendo da aplicação, 24 segundos pode ser um prazo razoável, mas eventualmente pode ser inaceitável. Assim sendo, mesmo que a análise de perfil de usuários mostre que um link de 2 Mbps atende a necessidade geral, fatores

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Utilizar o método de cálculo de dimensionamento apresentado nesta OT para estimar a largura da banda de internet.
- Documentar os perfis de usuário que não estejam presentes nesta OT.
- Considerar se há transmissões em burst (método de transferência de dados no qual as informações são reunidas e enviadas como uma unidade, propiciando transmissões em alta velocidade) que sejam relevantes ou até mesmo imprescindíveis no negócio para o dimensionamento do tamanho da banda e incorporá-las no cálculo da banda.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Trabalhar com uma margem de segurança e implementar um percentual de acréscimo ao valor final encontrado no cálculo, para se ter escalabilidade, bem como acomodar melhor eventuais picos no uso da rede.

[OT 007]
BACKUP E ARMAZENAMENTO DE DADOS

31 CONSIDERAÇÕES GERAIS SOBRE BACKUP

34 LOCAIS DE ARMAZENAMENTO DE BACKUP

38 FORMAS E TIPOS DE BACKUP

42 TESTES, RETENÇÃO E RESTAURAÇÃO DE BACKUP

43 DIRETRIZES DE BACKUP PARA DATA CENTERS PRÓPRIOS

45 ARMAZENAMENTO DE DADOS

46 REFERÊNCIAS

Faz considerações a definições gerais sobre cópia de segurança de dados e pretende estimular a implantação de políticas de Backup nos Órgãos Setoriais. Para tanto, o texto traz recomendações e sugestões a respeito de locais de armazenamento, formas e tipos de Backup, testes, retenção e restauração da cópia de segurança e define diretrizes de Backup para Data Centers próprios. Vale ressaltar que não é objetivo deste documento o uso de armazenamento de dados em mídias físicas que não se relacionem diretamente com a Tecnologia da Informação e Comunicação como papel, microfilme e tab-jacks por exemplo.

CONSIDERAÇÕES GERAIS SOBRE BACKUP

O backup, ou a cópia de segurança dos dados, deve ser considerado como a última linha de defesa de proteção dos dados. Desta forma, o backup não prescinde das demais medidas relativas à segurança da informação, sejam elas boas práticas de mercado ou dispostas em outras Orientações Técnicas. Tais medidas incluem aspectos como conscientização de usuários, atualização de sistema operacional e uso de antivírus, entre muitas outras possibilidades.

Além do viés de segurança, o backup também pode ser utilizado para recuperação de versões anteriores de arquivos e dados, bem como o arquivamento de dados raramente alterados e pouco acessados.

O Órgão Setorial é responsável pela gestão dos seus backups, bem como da sua política de backups.

O backup deve ser planejado para que seja coerente com as necessidades do Órgão Setorial, visando ter adequada segurança dos dados e alinhamento aos objetivos e realidades do Órgão. Caso contrário, corre-se o risco de ter gastos e esforços operacionais desnecessários.

Existem quatro perguntas fundamentais para o backup:

1) O que copiar?
2) Onde copiar?
3) Quando copiar?
4) Como copiar?

As respostas para essas perguntas moldarão a política de backup do Órgão Setorial. As seções subsequentes explorarão alguns aspectos a serem considerados sobre as questões acima.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Definir, documentar e divulgar a política de backup para o Órgão Setorial, estabelecendo procedimentos alinhados com as suas necessidades e objetivos.
- Explicitar na política de backup as respostas para as quatro questões fundamentais de backup: o que, onde, quando e como.
- Realizar uma ou mais cópias de segurança para os seguintes dados, no mínimo:
  - Imagem do sistema
    - Incluindo o sistema operacional, os programas padrão instalados, configurações e arquivos padrão dos usuários.
  - Dados realmente importantes
    - A análise da importância dos dados deve ser feita no contexto das atividades de negócio do Órgão Setorial, visto que o mesmo dado pode ter importâncias diferentes para Órgãos diferentes, e suas conclusões devem estar refletidas na política de backup.
- Realizar o backup com foco nos dados ou arquivos corporativos e não nos arquivos pessoais dos usuários.
  - Dados ou arquivos corporativos são aqueles utilizados, ou que impactam, nas atividades do Órgão Setorial.
    - Para esta classificação, o Órgão Setorial deverá adotar a supremacia da essência sobre a forma. Desta forma, arquivos alegados como pessoais devem ser considerados como corporativos, se eles impactarem nas atividades do Órgão Setorial.
- Não realizar o backup de arquivos que possam conter códigos maliciosos nem de arquivos que possam ter sido modificados/substituídos por agentes externos não autorizados.
  - Exceção feita a backups feitos especificamente para propósitos de segurança da informação, que podem ser executados apenas por Órgãos Setoriais de nível de

maturidade igual ou superior à Série C e que possuam servidor formalmente capacitado em Segurança da Informação ou que possuam uma unidade administrativa formal voltada especificamente à Segurança da Informação.

- Considerar as disponibilidades técnicas, físicas, orçamentárias e de pessoal para a elaboração e atualização da política de backup.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Investir na capacitação dos servidores de TIC do Órgão Setorial para aprimorar e atualizar os seus conhecimentos sobre as diversas possibilidades e tecnologias de backup.
- Evitar o backup de arquivos binários (executáveis e bibliotecas), pois podem conter arquivos maliciosos[4] ou corrompidos, que acabarão sendo recuperados em caso de restauração de backup.
- Criar uma ou mais listas de arquivos que não serão objeto de backup.
- Fazer o backup apenas dos dados confiáveis.

4. Os arquivos podem ser tanto danosos (vírus, cavalos de Troia, ransomware e demais tipos de malware) quanto programas potencialmente indesejados (adware, etc.).

LOCAIS DE ARMAZENAMENTO E BACKUP

Os backups podem ser armazenados tanto offline quanto online.

Backups offline incluem mídias como pendrive, CD, DVD, Blu-Ray, disco (interno ou externo), cartão de memória (SD, miniSD, microSD, SDHC etc.), fita, etc. Além disso, podem ser feitos no próprio local (on site) ou remotamente (off site).

Backups online incluem ambientes como discos de rede (tanto NAS quanto SAN), datacenter e nuvem (privada ou pública).

Em particular, é necessário atentar para a diferença entre o armazenamento na nuvem e o backup na nuvem. O armazenamento na nuvem pode ser usado para fins de backup, mas não necessariamente realiza backup dos arquivos armazenados .

Para mídias offline, é essencial considerar o tempo de vida útil. Mídias que excederem esse tempo podem continuar funcionais, mas a chance de sofrerem com a degradação passa a ser relevante.

No âmbito desta Orientação Técnica, o tempo estimado de vida útil das mídias offline pode ser consultado na tabela a seguir, considerando-se seu armazenamento e manuseio em condições adequadas. Mídias não contempladas na tabela podem ser consideradas como tendo vida útil indeterminada.

Além disso, os Órgãos Setoriais estão desobrigados de realizar a recuperação de dados armazenados em mídias obsoletas, exceto para dados críticos ao negócio, assim identificados pelo responsável pela área de TIC do Órgão Setorial.

TIPO DE MÍDIA	TEMPO ESTIMADO DE VIDA ÚTIL
Cartões perfurados	Obsoleto, não se recomendando seu uso
Disquetes (5¼, 3½, Zip disk etc.)	Obsoleto, não se recomendando seu uso
LDs e MDs	Obsoleto, não se recomendando seu uso
CDs e DVDs	2 (dois) anos
Disco rígido (HD) magnético[5]	4 (quatro) anos
Blu-Ray	5 (cinco) anos
Memória flash (pendrives, cartões de memória etc.)	5 (cinco) anos
Disco rígido (HD) de estado sólido (SSD)	5 (cinco) anos
NAS (Network Attached Storage)	5 (cinco) anos ou a garantia do fabricante, o que for maior
SAN (Storage Area Network) baseado em HD	5 (cinco) anos ou a garantia do fabricante, o que for maior
Fitas/Cartuchos magnéticos	10 (dez) anos
M-Disc	20 (vinte) anos

Tabela 9: Tempo estimado de vida útil das mídias offline[6].

Para backup offline, a armazenagem das midias físicas também é um aspecto importante a ser considerado, de forma a mitigar eventuais danos por condições ambientais e/ou manuseio humano inadequado.

Ainda, é relevante considerar a questão de escolher entre adotar um backup on site ou off site, incluindo o caso de backup na nuvem. A tabela a seguir mostra o cenário de uso mais apropriado para cada abordagem.

5. Entende-se neste caso como o HD doméstico, seja externo ou interno.

6. Adaptado de https://www.storagecraft.com/blog/data-storage-lifespan/ e http://www.popularmechanics.com/technology/gadgets/how-to/g1007/how-long-will-your-discs-and-drives-last/

LOCAL DO BACKUP	CENÁRIO APROPRIADO
On site	Recuperação rápida de dados, especialmente se for para pedidos de baixo volume de dados ou para locais de baixa velocidade de conexão (largura de banda de rede).
Off site	Maior necessidade de reduzir o risco de perda de dados em caso de problemas nas instalações físicas do site (local) principal.
Off site - nuvem	Mesmo cenário para o caso off site, mas para casos em que há conexão adequada com a internet e não há disponibilidade/viabilidade de ter um site físico para backup.

Tabela 10: Cenários mais apropriados de uso para diferentes locais de backup.

Para o caso de backup na nuvem, devem-se considerar, no mínimo, os seguintes fatores para a sua contratação:

1) Sistemas suportados pelo fornecedor;
2) Processos disponíveis de backup e restauração e suas interfaces de usuário;
3) Possibilidade de automatização de processos de backup e restauração;
4) Espaço de armazenagem;
5) Restrições de arquivos em termos de tamanho e tipo;
6) Período de retenção de dados;
7) Políticas de privacidade e segurança dos dados;
8) Níveis de suporte oferecidos;
9) Condições relativas à transferência de dados quando do encerramento do contrato.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Escolher os locais de armazenamento de backup, bem como os tipos de mídia, considerando-se o cenário, a criticidade dos dados e as instalações físicas disponíveis.
- Não utilizar mídias obsoletas, por causa da dificuldade de se adquirir leitores e/ou recuperar as informações gravadas nelas.
- Utilizar mídias que estiverem dentro da sua vida útil.
- Quando a mídia original estiver se aproximando do fim da sua vida útil, realizar a cópia integral do backup para uma nova mídia, após sua validação com relação à integridade dos dados.
- Identificar as mídias de armazenamento offline de forma que facilitem a recuperação do dado desejado.
- Armazenar as mídias em local com acesso controlado e acondicioná-las de modo a mitigar a ação de agentes nocivos naturais, notadamente poeira, luz, calor e umidade.
- Para armazenamento off site, avaliar a adequação do link de rede às necessidades de backup e recuperação de dados.
- Para armazenamento off site na nuvem, considerar os diferentes fatores para sua contratação (conforme acima) e implantar uma política de segurança para gestão de usuários e senhas com acesso ao backup na nuvem.
- Para armazenamento e backup off site na nuvem, garantir com o provedor de serviço de armazenamento que o servidor destino do backup esteja localizado em país que possua uma Lei de proteção de dados pessoais no mínimo equivalente à 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).
- Adotar políticas de descarte de mídias para mitigar o risco de exposição indesejada de dados.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Etiquetar e nomear as mídias offline com informações que facilitem a sua localização, constando, por exemplo, um identificador único, o tipo do dado armazenado e a data de gravação.
- Utilizar uma base de dados ou um sistema para realizar a gestão das mídias offline.
- Para o descarte de mídias, avaliar medidas como destruição lógica dos dados (ex: formatação em baixo nível) ou até mesmo a destruição física da mídia (ex: fragmentação física do Blu-Ray).
- Para backup na nuvem, avaliar a adoção de autenticação de dois fatores.

FORMAS E TIPOS DE BACKUP

Uma das grandes definições a serem tomadas com relação ao backup é a quantidade de cópias a serem mantidas.

Os Órgãos Setoriais possuem autonomia para buscar a forma que melhor atende às suas necessidades. Como ponto de partida, pode-se citar a Regra 3-2-1, que preconiza a geração de pelo menos 3 (três) cópias dos dados (uma primária e dois backups), que devem ser armazenadas em pelo menos 2 (duas) mídias diferentes, sendo que 1 (uma) das cópias deve ser off site ou ao menos offline.[7]

Outra definição que deve ser tomada é o tipo de backup e a periodicidade com que ela deve ser feita.

Existem quatro tipos de backup, elencados na tabela a seguir.

7. Outras formas de backup utilizados que podem ser citadas são: Backup to Disk, then data moved to tape (D2D2T), Backup to Disk (D2D), Backup to Disk, then data moved to lower tier of disk (D2D2D), Backup to tape (D2T), Backup to disk, then data moved to cloud (D2D2C) e Backup to cloud (D2C).

Tipo	Descrição	Vantagens	Desvantagens
Completo	Copia todos os dados; Serve como referencial para os demais tipos	Mais básico e completo; Cópia de todos os dados em um único conjunto de mídia; Recuperação simples	Mais demorado; Ocupa mais espaço
Incremental	Copia apenas os dados alterados ou criados após o último completo ou incremental	Menor volume de dados; Mais rápido; Ocupa menos espaço de armazenamento	Recuperação mais complexa (primeiro um completo e depois todos os incrementais)
Diferencial	Copia os dados alterados ou criados desde o último backup completo	Recuperação mais rápida que o incremental (precisa só do último completo enquanto o incremental precisa do completo e dos incrementais)	Ocupa mais espaço que o incremental e menos que o completo; gasta mais tempo que o incremental e menos que o completo
Progressivo	Similar ao incremental mas com maior disponibilidade dos dados	Recuperação automatizada e mais eficiente (não precisa descobrir os conjuntos a serem recuperados)	Recuperação mais lenta que o diferencial e o completo (precisa analisar diferentes conjuntos para terminar o processo)

Tabela 11: Comparativo dos diferentes tipos de backup1.

7. Retirado de Backup - o básico cada vez mais essencial – Cert.br, 06/2017.

Já a periodicidade se refere à frequência de geração ou atualização de backups e deve ser estabelecida com base no apetite ao risco da perda de dados, considerando-se que, quanto maior a frequência das cópias, menor será a perda de dados, mas maiores serão os gastos e mais complexa poderá ser a recuperação.

Além de backups periódicos, o Órgão Setorial poderá realizar backups extemporâneos, sempre que entender que há algum risco iminente, que pode incluir eventos como, por exemplo:

- mau funcionamento;
- mensagens de logs e consoles de monitoramento sobre falhas;
- alteração/atualização de sistemas;
- envio a serviços de manutenção; e
- incidentes de segurança da informação.

A política pode também estabelecer metas de RPO (Recovery Point Objective) e RTO (Recovery Time Objective), conforme as necessidades de negócio.

Para fins desta Orientação Técnica, define-se o RPO como o intervalo de tempo aceitável entre o momento do último backup do dado e o momento da falha .

Por outro lado, o RTO é o intervalo de tempo necessário para a restauração de um processo sem comprometer a continuidade de negócio . Tanto o RPO quanto o RTO podem ser incorporados dentro de níveis de serviço.

Outra questão relevante é a segurança do backup. Além das questões físicas de integridade das mídias, deve-se considerar a segurança lógica dos dados, especialmente em termos de confidencialidade e integridade.

Em termos de procedimentos operacionais de geração de backup, o Órgão Setorial poderá fazer de forma manual ou automatizada, conforme as necessidades e realidades do Órgão, podendo inclusive utilizar ferramentas, seja de mercado ou desenvolvidas, para essa finalidade.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Criptografar backups de dados potencialmente sensíveis ou não classificados como público conforme a legislação vigente relativa ao acesso à informação.

  ■ Utilizar algoritmos considerados matematicamente seguros para a criptografia, evitando o uso de algoritmos considerados como fragilizados ou quebrados matematicamente .

- Quando tecnicamente viável, realizar backup dos dados corporativos gerados, mantidos ou geridos pelo usuário quando houver razoável certeza de que ele será removido, cedido, exonerado ou demitido, visando mitigar o risco da perda de dados relevantes.

- Definir uma lista de riscos iminentes, que ensejam a realização de um backup extemporâneo dos dados.

- Realizar backup dos dados relevantes quando forem identificados um ou mais riscos iminentes para os dados.

- Realizar periodicamente um backup completo dos dados e backups de outros tipos entre dois backups completos, visando mitigar o risco da perda de dados.

- Para os backups periódicos, utilizar ferramentas que automatizem o processo, parcial ou totalmente, para reduzir a ocorrência de erros manuais e ganhar maior aderência à

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Realizar um backup completo no mínimo uma vez por mês, se possível uma vez por semana, e os outros tipos de backup no mínimo uma vez por semana, se possível uma vez por dia.

- Gerar e armazenar as informações relativas à integridade dos dados de backup (checksum ou hash), realizando-se a sua conferência quando da sua recuperação.

- Definir RPO e RTO para dados de maior criticidade.
- Definir RPO e RTO dentro de acordo de níveis de serviço (SLA – Service Level Agreement) em caso de contratação de um prestador de serviços de backup.

TESTES, RETENÇÃO E RESTAURAÇÃO DE BACKUP

Para que o backup atenda às suas finalidades, é necessário considerar um procedimento de teste e verificação da sua integridade e legibilidade. Caso contrário, corre-se o risco de encontrar problemas como dados corrompidos e mídias ou formatos obsoletos. Esses procedimentos devem ser feitos periodicamente para detectar preventivamente potenciais fontes de risco e não apenas para fins de auditoria.

Um outro fator a ser considerado no backup é a retenção de dados, ou seja, por quanto tempo eles devem ser armazenados. Deve-se considerar as tabelas de temporalidade de dados em vigor , bem como outras obrigações legais (compliance), a disponibilidade de espaço de armazenamento, seja físico ou lógico, e a disponibilidade orçamentária-financeira.

A restauração do backup é um procedimento para recuperar os dados após uma falha e deve estar contida dentro do plano de backup.Ela pode ser tanto total (restauração integral dos dados) ou parcial (restauração apenas de uma porção limitada de dados).

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Incluir um ou mais procedimentos de verificação de backups na política de backup, contendo no mínimo uma verificação pontual, quando da geração do backup, e uma rotina de verificação periódica.

- Em caso de contratação de serviços de backup, incluir um plano de saída no contrato, para manter a continuidade de serviço quando do encerramento do contrato.
- Testar os backups antes da sua restauração.

DIRETRIZES DE BACKUP PARA DATA CENTERS PRÓPRIOS

Para Data Centers próprios, ou seja, de propriedade do Órgão Setorial, esta Orientação Técnica define mais algumas diretrizes, além das já apresentadas nas outras seções.

A primeira diretriz versa sobre backup de sistemas de bancos de dados. Divididos tipicamente em camada de apresentação, negócios e dados, tais sistemas apresentam maior complexidade de backup para a camada de dados, que normalmente está armazenado em um Sistema Gerenciador de Banco de Dados. Para eles, os Gerenciadores possuem, via de regra, dois modelos de backup: lógico e físico.

O backup lógico é através do export ou dump das informações em arquivos texto. O backup físico é feito através utilitários específicos, que fazem o backup de arquivos binários em um formato proprietário que deve ser restaurado pelo próprio utilitário.

A tabela a seguir descreve de forma sucinta as duas possibilidades:

Backup de BD	Características	Cenário ideal
Lógico	Permite escolha granular dos dados a serem recuperados; A recuperação pode ser em ambientes diferentes do original	Armazenamento por longos períodos e/ou recuperação de dados em um ambiente diferente do original.
Físico	Monolítico; Exige o mesmo ambiente de quando o backup foi feito	Recuperação rápida e/ou integral de dados para um ambiente que não sofreu modificações

Tabela 12: Comparativo dos dois tipos de backup de Banco de Dados.

A outra diretriz é para serviços de missão crítica, que exige uma continuidade de negócios bastante rigorosa, com RPO e/ou RTO próximos a zero. Para este caso, a diretriz básica é adotar o uso de um ou mais servidores espelho com sincronização constante.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Realizar o backup dos sistemas de bases de dados, sendo que a camada de dados deve ter backup lógico e/ou físico.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Realizar o backup lógico e físico da camada de dados e escolher o que melhor se adequa à situação para a restauração do backup.
- Em relação ao processo de backup, não realizar a sincronização constante de forma automática de remoções, pois podem levar a remoções indesejadas de dados.

ARMAZENAMENTO DE DADOS

Os Órgãos Setoriais possuem autonomia para buscar a forma que melhor atende às suas necessidades e disponibilidades, de forma que a sua política interna de armazenamento de dados seja exequível e efetiva.

Em particular, o uso de serviços na nuvem para armazenamento apresenta considerações próprias, incluindo questões de segurança da informação. Para informações específicas sobre serviços de nuvem, devem-se consultar as Orientações Técnicas para computação em nuvem.

Além disso, cuidados básicos de redundância de dados devem estar presentes para Órgãos Setoriais que mantenham Data Centers próprios.

Por fim, para armazenamento de código-fonte e/ou de documentos, o uso de ferramentas de versionamento passa a ser bastante interessante, para que se tenha maior rastreabilidade e consistência nos dados.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Adotar redundância de dados em multiplos discos físicos utilizando tecnologia RAID ou similar.
- Adotar como diretriz básica o armazenamento dos dados corpoativos em diretórios compartilhados na rede, quando estes existirem, para facilitar o acesso aos dados .
- Criar diretórios (pastas) específicas com restrições de acesso para armazenamento de dados sensíveis.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Avaliar o uso de ferramentas de sincronização e compartilhamento de dados.
- Avaliar o uso de ferramentas de gestão e auditoria de dados, visando ter melhor visibilidade e rastreabilidade.
- Considerar o uso de ferramentas de versionamento para documentos e códigos-fonte.

REFERÊNCIAS

"Backup Site", in Wikipedia. Website, disponível em <https://en.wikipedia.org/wiki/Backup_site>.

"Dispositivo de armazenamento", in Wikipedia. Website, disponível em <https://pt.wikipedia.org/wiki/Dispositivo_de_armazenamento>.

"Recovery Point Objective", in Wikipedia. Website, disponível em <https://en.wikipedia.org/wiki/Recovery_point_objective>.

"Recovery Time Objective", in Wikipedia. Website, disponível em <https://en.wikipedia.org/wiki/Recovery_time_objective>

Cert.br. "Backup - o básico cada vez mais essencial". ZUBEN, Miriam von. Publicado em jun/2017.

Cert.br. "Cartilha de segurança para a Internet - Mecanismos de Segurança". Website, disponível em <https://cartilha.cert.br/mecanismos/>

Gartner, Inc. "Designing a Storage Strategy Document". ANTELMI, Joseph. Publicado em 22/01/2016.

Gartner, Inc. "Discover the Truth About the Use of Disk, Tape and Cloud Backup". RHAME, Robert; RUSSEL, Dave. Publicado em 27/03/2017.

Gartner, Inc. "How to Address Three Key Challenges When Considering Endpoint Backup". RINNEN, Pushan. Publicado em 19/01/2016.

[OT 008]
ACESSIBILIDADE DIGITAL NA ADM. MUNICIPAL

48 ACESSIBILIDADE DIGITAL
na administração pública

51 CRIANDO UM SÍTIO OU PORTAL ACESSÍVEL

55 PRATICAS DE DESENVOLVIMENTO

55 MANUTENÇÃO DA ACESSIBILIDADE

56 ANEXO

61 REFERÊNCIAS

Aborda as principais situações vividas por usuários com deficiência, e tem a finalidade de definir diretrizes de forma a suprimir obstáculos no acesso internet para pessoas com deficiência, trazendo tópicos que informam a respeito de como se cria um site acessível, enunciam algumas sugestões sobre práticas de desenvolvimento de portais e recomendações para a manutenção da acessibilidade como um processo contínuo na administração municipal. Traz também uma lista de critérios para a verificação da acessibilidade Web como anexo.

ACESSIBILIDADE DIGITAL

na Administração Pública

Podemos considerar acessibilidade digital como a supressão de obstáculos na Web, de forma que os sítios e portais sejam projetados a fim de que todas as pessoas possam perceber, entender, navegar e interagir de maneira efetiva com as páginas.

Nas últimas décadas, a expansão da Internet vem revolucionando as formas de comunicação, de acesso à informação e de realização de negócios em todo o mundo.

Um dos aliados das pessoas com deficiência para o uso do computador são os recursos de tecnologia assistiva, que auxiliam na realização de tarefas antes muito difíceis ou impossíveis de realizar, promovendo, desta maneira, a autonomia, independência, qualidade de vida e inclusão social de pessoas com deficiência.

Apesar de sua enorme importância na promoção da acessibilidade às pessoas com deficiência, os recursos de tecnologia assistiva, por si só, não garantem o acesso ao conteúdo de uma página da Web. Para tal, é necessário que a página tenha sido desenvolvida de acordo com os padrões Web (Web Standards) e as recomendações de acessibilidade, os quais serão abordados ao longo desta Orientação.

No que se refere a acesso ao computador, as quatro principais situações vivenciadas por usuários com deficiência são:

- Acesso ao computador sem mouse: no caso de pessoas com deficiência visual, dificuldade de controle dos movimentos, paralisia ou amputação de um membro superior;
- Acesso ao computador sem teclado: no caso de pessoas com amputações, grandes limitações de movimentos ou falta de força nos membros superiores;
- Acesso ao computador sem monitor: no caso de pessoas com cegueira;

- Acesso ao computador sem áudio: no caso de pessoas com deficiência auditiva.

No âmbito da Prefeitura do Município de São Paulo, a inacessibilidade de sítios e portais eletrônicos exclui uma parcela significativa da população do acesso aos serviços e informações veiculadas nos sites da Administração Municipal.

Além do acesso às páginas institucionais, alguns serviços podem ser realizados pela internet, por exemplo: marcação de exame médico, poda de árvore, conserto de calçadas, agendamento eletrônico para cadastro no ISS(Imposto Sobre Serviços), ver o itinerário de ônibus, ver a programação cultural da cidade, escolher o local mais próximo para vacinar seu animal de estimação, solicitar a retirada de entulho, tapa-buracos, e outros serviços.

Com a finalidade de promover a transformação social necessária à inclusão das pessoas com deficiência e mobilidade reduzida, a Secretaria Municipal da Pessoa com Deficiência (SMPED) foi criada pela Lei nº 14.659, de 26 de dezembro de 2007.

A Secretaria tem como missão promover a transformação social necessária à inclusão das pessoas com deficiência e mobilidade reduzida. Assim, compete a ela conduzir, executar e articular as ações governamentais entre os órgãos e entidades da Prefeitura do Município de São Paulo e os diversos setores da sociedade, visando à implementação da política municipal para as pessoas com deficiência e mobilidade reduzida.

A SMPED tem a função, ainda, de desenvolver projetos destinados à implementação das políticas públicas com o objetivo de melhorar a qualidade de vida da pessoa com deficiência – seja ela física, intelectual, auditiva, visual, múltipla, surdocegueira - ou com mobilidade reduzida.

Dentro da estrutura básica da SMPED, importante ressaltar

a Comissão Permanente de Acessibilidade (CPA), órgão colegiado composto por representantes de diversas secretarias, órgãos municipais e sociedade civil, com o objetivo de elaborar "normas e controle que garantam a acessibilidade para pessoas com deficiência ou com mobilidade reduzida a edificações, vias e espaços públicos, transportes, mobiliário e equipamentos urbanos, bem como aos meios de divulgação de informações e sinalizações relativas à acessibilidade".

No tocante à Acessibilidade Digital, especificamente, o Decreto Municipal nº 49.063/07 instituiu o Selo de Acessibilidade Digital (SAD) com o propósito de certificar a acessibilidade nos sítios e portais da internet, tanto no tocante à disponibilização de conteúdo quanto ao acesso a ferramentas e serviços virtuais, cuja competência de emissão é da CPA.

O Selo de Acessibilidade Digital possui validade de 1 (um) ano e será concedido aos sítios ou portais mantidos por órgãos municipais e por pessoas físicas ou jurídicas com sede ou representação no Brasil que atenderem os critérios e procedimentos para a sua concessão, conforme estabelecidos em Portaria específica a ser publicada.

Dentre as exigências para obtenção do Selo de Acessibilidade Digital, destacam-se: possuir percentual de aderência de, no mínimo, 95% do Modelo de Acessibilidade em Governo Eletrônico – eMAG e cumprir os critérios da lista de verificação para análise manual (ANEXO I).

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Requerer a concessão do Selo de Acessibilidade Digital por meio eletrônico, através do Portal 156, contendo os documentos estabelecidos em Portaria específica.

CRIANDO UM SÍTIO OU PORTAL ACESSÍVEL

O desenvolvimento de um sítio ou portal com acessibilidade digital depende de vários fatores, tanto aspectos relacionados ao desenvolvimento quanto diretrizes específicas voltadas para publicadores de conteúdo.

Por exemplo, a adição do equivalente textual, pelos publicadores de conteúdo, às imagens informativas que sejam exibidas em artigos e notícias é pré-requisito que deve ser seguido concomitantemente à adoção dos padrões WEB, pelos desenvolvedores.

No tocante ao desenvolvimento de um sítio acessível, existem basicamente três grandes passos:

SEGUIR OS PADRÕES WEB DO W3C

O World Wide Web Consortium (W3C) é a principal organização de padronização da Web, consistindo em um consórcio internacional com quase 400 membros, incorporando empresas, órgãos governamentais e organizações independentes com a finalidade de estabelecer padrões para a criação e a interpretação de conteúdos para a Web.

Os Padrões Web recomendados pelo W3C têm como objetivo principal orientar os desenvolvedores para o uso de boas práticas que tornam os benefícios da Web disponíveis a todos, sem exceção, independente de hardware, software, infraestrutura de rede, idioma, cultura, localização geográfica, habilidade física e mental.

Uma página desenvolvida de acordo com os padrões Web deve estar em conformidade com as normas HTML, XML, XHTML e CSS, seguindo as regras de formatação sintática.

Segundo o W3C, utilizar padrões no momento de desenvolver um site tem como objetivos, dentre outros:

- Comportamentos sofisticados que funcionam em vários navegadores e plataformas.
- Acessibilidade sem acabar com a beleza, o desempenho ou a sofisticação.
- Suportar dispositivos não tradicionais, desde aparelhos portáteis até leitores braile ou leitores de vídeos usados por pessoas com deficiência, sem o incômodo e o custo de criar versões separadas.
- Separar a apresentação do conteúdo e comportamento, permitindo designs criativos, apoiados numa estrutura rigorosa dos documentos e permitindo a reutilização dos documentos Web.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- A partir da publicação desta Orientação, utilizar os padrões HTML e CSS conforme preconizados pelo W3C (http://www.w3c.br/Padroes/) nos novos desenvolvimentos, inclusive contratado, de quaisquer sítios ou portais para a Prefeitura do Município de São Paulo.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Remodelar os sítios ou portais desenvolvidos anteriormente à publicação desta Orientação, de forma a satisfazer os Padrões WEB preconizados pelo W3C (http://www.w3c.br/Padroes/).

SEGUIR AS DIRETRIZES E RECOMENDAÇÕES DE ACESSIBILIDADE

Atualmente existem vários documentos internacionais que propõem regras, ou normas de acessibilidade para a web. Todos, no entanto, baseiam-se em diretrizes do W3C.

A principal documentação nessa área é a WCAG (Web Content Accessibility Guidelines), padrão internacional desenvolvido pelo consórcio W3C a partir da criação do WAI (Web Accessibility Initiative), contendo as recomendações de acessibilidade para conteúdo Web.

Entretanto, com a finalidade de adoção progressiva das recomendações de acessibilidade elencadas no WCAG, listaremos a seguir as que se revestem de caráter obrigatório para os órgãos da Administração Municipal.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

Atender, no mínimo, para o desenvolvimento de novos sítios ou portais, que:

- Toda imagem informativa que é exibida ao usuário tenha uma alternativa textual que serve a um propósito equivalente;
- A cor não é utilizada como o único meio visual de transmitir informações, indicar uma ação, pedir uma resposta ou distinguir um elemento visual;
- Toda a funcionalidade do sítio ou portal é operável através de uma interface de teclado;
- As páginas web não incluem nenhum conteúdo que pisque mais de três vezes no período de um segundo;
- As páginas web têm títulos que descrevem o tópico ou a finalidade;
- É fornecido uma explicação para siglas, abreviaturas e palavras incomuns;
- O idioma principal da página está identificado;e
- As páginas não possuem atualização ou redirecionamento automático.
- As fontes das páginas possuem tamanho ideal de leitura (11 ou superior).

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Adotar, de forma a complementar as recomendações anteriores, modelos e normas específicos sobre acessibilidade digital nos sítios ou portais, tais como as últimas versões do WCAG e eMAG.

REALIZAR A AVALIAÇÃO DE ACESSIBILIDADE

Após o desenvolvimento do sítio ou portal de acordo com os padrões Web e as recomendações de acessibilidade, é necessário verificar se os objetivos de acessibilidade foram efetivamente atingidos.

Inicialmente, uma validação automática pode ser realizada através de softwares ou serviços online que ajudam a determinar se foram respeitadas ou não as recomendações de acessibilidade, gerando um relatório de não conformidades.

Em que pese a avaliação de acessibilidade automática tornar mais rápida e menos trabalhosa a verificação, os validadores automáticos, por si só, não determinam se um sítio está ou não acessível.

Para uma avaliação efetiva, é conveniente uma posterior validação manual e, por fim, testes com usuários reais.

Pode-se resumir a avaliação de acessibilidade nos seguintes passos:

- A. Validar os códigos do conteúdo HTML e das folhas de estilo (CSS): Alguns validadores de HTML (https://validator.w3.org/) e CSS (https://jigsaw.w3.org/css-validator/) são disponibilizados pela própria W3C, responsável por manter a padronização das linguagens.
- B. Verificar o fluxo de leitura da página: A forma mais simples é inibir o CSS, imagens e scripts, lendo apenas o HTML da página. Boa parte dos navegadores possuem ferramentas ou extensões que permitem essa visualização. Outra opção é utilizar navegadores textuais, como o Lynx ou um leitor de tela.

- C. Realizar a validação automática de acessibilidade utilizando o ASES WEB: O ASES WEB pode acessado por meio do sítio http://asesweb.governoeletronico.gov.br/ases.
- D. Realizar a validação manual: Os validadores automáticos não são capazes de detectar todos os problemas de acessibilidade em um sítio, pois muitos aspectos requerem um julgamento humano, necessitando de uma validação manual.Por exemplo, validadores automáticos conseguem detectar se o atributo para descrever imagens foi utilizado em todas as imagens do sítio, mas somente uma pessoa poderá verificar se a descrição da imagem está adequada ao seu conteúdo.
- E. Teste com usuários reais: Por fim, a realização de testes com usuários reais (pessoas com deficiência ou limitações técnicas) torna-se adequado. Um usuário real poderá dizer se um sítio está realmente acessível, compreensível e com boa usabilidade e não simplesmente tecnicamente acessível.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Realizar a validação automática através do ASES WEB (http://asesweb.governoeletronico.gov.br/ases), buscando efetuar as correções das eventuais não conformidades.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Atestar que os sítios ou portais de responsabilidade do órgão estejam em conformidade com o relatório disponibilizado pelo ASES WEB (http://asesweb.governoeletronico.gov.br/ases).
- Constatar que os critérios estabelecidos na lista de verificação para análise manual (ANEXO I) estão sendo atendidos.
- Contemplar a verificação com usuários reais, de forma a mensurar as dificuldades e efetuar as correções.

DAS PRÁTICAS DE DESENVOLVIMENTO

Algumas práticas de desenvolvimento de sítios e portais podem configurar obstáculo para a acessibilidade digital e, também, para uma boa experiência de usabilidade quando se utiliza dispositivo móvel.

QUAIS SÃO AS NOSSAS SUGESTÕES?

Evitar o uso das seguintes práticas no desenvolvimento de sítios ou portais:

- Uso de animações e aplicações FLASH;
- Uso de CAPTCHAS em formulários sem o equivalente auditivo;
- Tabelas para fins de diagramação;
- Elementos e atributos considerados depreciados pelo W3C. Exemplos: frame, applet, blink, marquee, basefont, center, dir, align, font, isindex, menu, strike, u, b, entre outros.

MANUTENÇÃO DA ACESSIBILIDADE

A manutenção da acessibilidade digital é um processo contínuo. Desta forma, recomenda-se que testes sejam realizados periodicamente em cada alteração de conteúdo e, em espaços determinados de tempo, validações globais.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Realizar testes de manutenção da acessibilidade, pelo menos em cada alteração de conteúdo, de forma a verificar se o sítio permanece acessível.

ANEXO

CRITÉRIOS E LISTA PARA VERIFICAÇÃO DA ACESSIBILIDADE WEB

As respostas às perguntas contidas na lista de verificação a seguir devem ser afirmativas (sim).

1. Navegação na página

Navegando pelos links do site com as teclas TAB (para avançar) e SHIFT + TAB (para voltar).

1.1 Após navegar no site do início ao fim sem utilizar o monitor (monitor desligado), sem clicar em nenhum link, é possível identificar o assunto de que se trata a página?

1.2 É possível utilizar a tecla TAB e as demais teclas do teclado sem impedimento e acessar todos os links da página?

1.3 O conteúdo dos links é claro e informa qual página será aberta?

1.4 Caso haja links adjacentes (sequência de links), estes estão separados explicitamente de forma que não há cacofonia (confusão ou extrema repetição), quando se ouve uma sequência longa de links?

1.5 Possui Outline (contorno que ressalte o elemento em foco) para destacar a navegação por tab?

2. Estrutura, navegação por cabeçalhos e por blocos de conteúdos

Os níveis de cabeçalho (elementos HTML H1 a H6) devem ser utilizados de forma hierárquica, pois organizam a ordem de importância e subordinação dos conteúdos, facilitando a leitura e compreensão. Pelo leitor de tela, deve ser possível navegar de um cabeçalho a outro e verificar a estrutura da página. A maioria dos leitores de tela utiliza o atalho "H" do teclado em combinação com os números de 01 a 06.

2.1 A hierarquia de cabeçalhos existe e está clara?

2.2 Os cabeçalhos estão ordenados e não há repetição do nível de cabeçalho <h1>?

2.3 A leitura e tabulação estão ordenadas de forma lógica e intuitiva?

2.4 Há âncoras para ir direto a um bloco de conteúdo como, por exemplo: o primeiro link da página é o "ir para o conteúdo principal"?

2.5 São utilizadas tabelas apenas para dados tabulares e não para efeitos de disposição dos elementos da página?

2.6 O título da tabela está definido e localizado no primeiro elemento da tabela?

2.7 Há um resumo dos dados de tabelas extensas e/ou é possível compreender a complexidade da tabela informacional?

2.8 Em tabelas de dados simples, estão associadas células de dados às células de cabeçalho?

2.9 Não há abertura de novas instâncias 'abas ou janelas' sem a solicitação do usuário?

2.10 Não há atualização automática periódica de páginas ('refresh') e nem redirecionamento automático de páginas (uma nova página que abre sem ser solicitada)?

2.11 Todas as funções da página são disponibilizadas via teclado e o foco não fica bloqueado ou fixado em um elemento da página?

2.12 Elementos que recebem o foco pelo teclado estão claramente marcados, ficando evidentes e passíveis de serem clicados?

2.13 Todos os scripts, conteúdos dinâmicos e outros elementos programáveis contidos nas páginas estão acessíveis e é possível sua execução via navegação?

2.14 Scripts, conteúdos dinâmicos e outros elementos programáveis (por exemplo: plugins de visualização de PDF, gráficos de pizza dinâmicos, entre outros) tem conteúdo/texto equivalente?

2.15 É possível acessar todo o conteúdo em lista e em seu(s) sub-nível(is)?

2.16 As cores do plano de fundo e do primeiro plano estão suficientemente contrastantes?

2.17 Não há utilização de efeitos visuais piscantes, intermitentes ou cintilantes?

2.18 O idioma principal da página está identificado?

2.19 Os elementos que possuem conteúdo em um idioma diferente do principal estão devidamente identificados?

2.20 Em resumo, é possível compreender a estrutura da página de forma que não gere confusão e se saiba qual informação será obtida ou quais ações e tarefas devem ser executadas com clareza?

2.21 As mensagens de erros geradas automaticamente pelo servidor (como, por exemplo, 404, 403 e 500) possuem acessibilidade com opção para voltar para a página anterior ou para a página inicial?

2.22 O Html5 foi desenvolvido seguindo os padrões da W3C e de forma semântica?

2.23 Foi adicionado Wai-aria em elementos dinâmicos e interface de controle? Exemplo: Carrossel com troca de slide.

2.24 Caso haja Pop-ups (moldais), estes são acessíveis?

2.25 As páginas são acessíveis e responsivas em dispositivos móveis?

3. Imagens acessíveis

Os testes abaixo visam verificar se os textos alternativos que descrevem as imagens lidas pelo software leitor de tela correspondem exatamente ao que as imagens mostram. Imagens que fazem parte do contexto da página (como um logotipo ou a foto que ilustra uma notícia) são consideradas imagens relevantes. Imagens decorativas, como fundo da página e bordas, não são consideradas relevantes.

3.1 Todas as imagens relevantes tem um texto alternativo claro e relacionado à imagem?

3.2 Na página, não existem imagens com texto (todos os textos estão em HTML)?

3.3 Há imagens mapeadas? Estão acessíveis?

3.4 Há infográficos? Estão acessíveis ou com texto equivalente?

3.5 Há gráficos de pizza ou gráficos de barra (outros tipos de conteúdo visual complexo)? Estão acessíveis ou com texto equivalente?

4. Preenchimento e navegação em formulários

Ao se navegar por formulários, não deve haver barreiras que impeçam que o usuário passe de campo em campo e acione botões. As instruções devem ser claras e os rótulos devem estar relacionados com cada campo. Os softwares leitores de tela devem ler cada campo e relacioná-lo com seu devido rótulo.

4.1 Os campos de formulário da página possuem um nome claro / compreensível?

4.2 As informações sobre o preenchimento dos formulários são claras, inclusive com informações sobre campos obrigatórios, que não devem usar somente cor para transmitir a informação (exemplo incorreto: "Campos obrigatórios estão marcados em vermelho")?

4.3 Estão claros quais campos são de preenchimento obrigatório?

4.4 Há alternativa em texto para os botões de imagem de formulários?

4.5 As etiquetas de texto (labels ou rótulos) estão associadas aos seus campos correspondentes no formulário?

4.6 Os campos dos formulários com informações relacionadas estão agrupados logicamente, e o propósito ou natureza dos agrupamentos está explicitado claramente?

4.7 Mensagens de erro e avisos são claros? É possível acessá-los facilmente?

4.8 Quando ocorre erro ou engano em alguma digitação, é possível corrigi-lo?

4.9 Quando ocorre erro ou engano em alguma digitação, é possível corrigi-lo?

4.10 Quando houver anti-spam para liberação de envio dos dados (captcha), estes itens estão disponíveis também em áudio e texto?

5. Tamanho e relacionamento de elementos

Verificação de problemas em relação ao tamanho dos elementos presentes no site. Elementos muito pequenos podem prejudicar o uso para muitas pessoas.

Utilize o Google Chrome, e a extensão "NoCoffee Vision Simulator", opção "Flutter (nystagmus)" definido em 100, para dificultar a interação com os elementos presentes na página e movimente o mouse sobre os menores links e elementos do site durante o teste.

5.1 É fácil clicar nos elementos da página?

5.2 O usuário é capaz de aumentar e diminuir o tamanho das fontes do site sem que o conteúdo ou a funcionalidade sejam perdidos? A técnica de "design responsivo" deve ser considerada para que o site se adapte ao tamanho da tela quando o usuário aumentar o tamanho das páginas (utilizando CTRL/COMMAND + para aumentar e CTRL/COMMAND - para diminuir).

5.3 O site se adapta adequadamente com zoom de 200%, exibindo as informações importantes e funcionalidades sem barras laterais de rolagem?

6. Conteúdo textual

6.1 Os textos contidos no site são de fácil compreensão e, para os textos de conhecimento mais avançados, estão disponibilizadas informações suplementares que expliquem ou ilustrem o conteúdo principal?

6.2 Na primeira ocorrência de siglas, abreviaturas ou palavras incomuns (ambíguas, desconhecidas ou utilizadas de forma muito específica), está disponibilizada sua explicação ou forma completa?

7. Legendas, transcrições e audiodescrição

Conteúdos em vídeo ou áudio devem ter alternativas textuais presentes na página. O usuário deve compreender o sentido das imagens em movimento e seus sons. Para conteúdos em vídeo com áudio (audiovisual), é necessária a inserção de legendas ou Closed Caption. Já para conteúdos informacionais apenas sonoros (exemplo: arquivo MP3), deve haver uma transcrição em texto.

7.1 Todos os vídeos ou áudios possuem alternativa em texto?

7.2 A alternativa textual possui o mesmo conteúdo que está sendo apresentado pelo vídeo ou pelo áudio?

7.3 Existe tradução para Libras em todo conteúdo de áudio e vídeo? Para conteúdos informacionais apenas no formato vídeo, é necessário que exista audiodescrição. Ela é responsável por informar os eventos, acontecimentos e outras informações visuais em forma de áudio.

7.4 Existe audiodescrição em todos os vídeos?

7.5 Há na página/site mecanismo para ativar, parar, pausar, silenciar ou ajustar o volume de qualquer som que se reproduza na página?

REFERÊNCIAS

eMAG 3.1 - Modelo de Acessibilidade em Governo Eletrônico

DECRETO MUNICIPAL Nº 39.651, DE 27 DE JULHO DE 2000

DECRETO MUNICIPAL Nº 49.063, DE 18 DE DEZEMBRO DE 2007

[OT 009]
AQUISIÇÕES DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

63 DEFINIÇÕES

64 COMPUTAÇÃO EM NUVEM

73 PREPARAÇÃO PARA ADOÇÃO DE SERVIÇO DE NUVEM

80 OPÇÕES DE SERVIÇOS DE NUVEM

86 ELABORAÇÃO DO EDITAL E TERMO DE REFERÊNCIA

95 REFERÊNCIAS

Tem como objetivo apresentar boas práticas em contratação e uso de serviços de computação em nuvem no âmbito da administração direta da Prefeitura do Município de São Paulo através de definições gerais a respeito dos benefícios do uso desse serviço. O documento também orienta sobre como se preparar para adotar um serviço de nuvem através de análise previa, traçando um plano de adoção do serviço, bem como apresentando uma análise de riscos envolvidos. Informa sobre opções de serviços considerando fornecedores e precificação. Por fim aborda a elaboração do edital de termo de referência para a contratação do Fornecedor de Nuvem, trazendo recomendações e sugestões a respeito de Cláusulas Críticas.

DEFINIÇÕES

Foram adotadas, dentro do escopo deste documento, as seguintes definições:

Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

Canal de Revenda de nuvem: na contratação de Fornecedores de nuvem, especialmente aqueles de grande porte, não raro haverá uma empresa atuando como canal de revenda associada a tal fornecedor, e servindo como intermediária entre o Fornecedor de nuvem e o Cliente da nuvem;

Cliente da nuvem: órgão/entidade setorial da administração municipal que está contratando o Fornecedor de nuvem;

Datacenter: o estabelecimento onde localiza-se a Nuvem, dotado de proteção e resfriamento apropriados para os dados e os equipamentos que os hospedam, e que conta com vários computadores servidores que processam e armazenam os dados dos Clientes.

Fornecedor de nuvem: empresa ou organização fornecedora de algum ou todos os componentes da computação em nuvem a outras empresas, organizações ou indivíduos. Neste documento, os termos "Fornecedor de nuvem", "Fornecedor de serviços de nuvem", "Provedor de nuvem", e "Provedor de serviços de nuvem" são tratados como sinônimos.

PDSTIC: Plano de Desenvolvimento Setorial de TIC, conforme definição do Artigo 13, inciso III do Decreto Municipal 57.653, de 07 de abril de 2017.

PETIC: Plano Estratégico de TIC, conforme definição do Artigo 13, inciso I do Decreto Municipal 57.653, de 07 de abril de 2017.

Portal de administração da nuvem: é a interface por meio da qual os Serviços de nuvem são ativados e gerenciados, e está acessível via internet. É através do Portal de administração da nuvem que serão exercidas as funções de controle dos Serviços de nuvem contratados.

Serviço de nuvem: empacotamento de recursos computacionais de modo eficiente para disponibilização para o Cliente por meio da nuvem, sob demanda, e abstraindo os recursos computacionais físicos subjacentes. Pode apresentar-se sob os modelos SaaS, PaaS, IaaS ou outros, e geralmente é cobrado de acordo com o uso, ao invés de ter o preço fixado. Neste documento, os termos "Serviço de nuvem" e "Serviço de computação em nuvem" são tratados como sinônimos.

SLA: Acordo de Nível de Serviço (Service Level Agreement), um acordo estabelecido em contrato que dispõe sobre o nível de serviço a ser fornecido por um Fornecedor de serviços a um Cliente, comumente usado em serviços relacionados à computação (como a computação em nuvem);

Valor do Ativo de Informação: valor, tangível e/ou intangível, que reflete tanto a importância do Ativo de Informação para atingir os objetivos estratégicos do Orgão ou entidade da Administração Municipal, quanto o quão cada Ativo de Informação é imprescindível aos interesses da sociedade e do Estado.

COMPUTAÇÃO EM NUVEM

Desde a publicação do Decreto Municipal 57.653, de 07 de abril de 2017, que define a Política Municipal de Tecnologia da Informação e Comunicação, a Prefeitura do Município de São Paulo tem buscado tornar seus departamentos mais ágeis e flexíveis por meio do uso das melhores práticas em Tecnologia da Informação e Comunicação. Dentre elas,

inclui-se o uso de Tecnologias de Informação e Comunicação baseadas em nuvem, ou simplesmente Computação em Nuvem (Cloud Computing).

Computação em nuvem é um modelo para permitir acesso por meio da rede, de modo ubíquo, conveniente e sob demanda a um agrupamento compartilhado de recursos computacionais compartilhados (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que possam ser rapidamente provisionados e liberados com mínimo esforço gerencial ou mínima interação do fornecedor dos serviços.

As características definidoras de uma nuvem são o amplo acesso por rede, a elasticidade rápida, os serviços mensurados, o auto-serviço sob demanda e o pooling (agrupamento) de recursos computacionais. Segue breve descrição destas características:

- amplo acesso por rede: as funcionalidades estão disponíveis por meio da internet e podem ser acessados por meio de mecanismos de rede padronizados, de modo a poderem ser utilizados a partir de diversas plataformas computacionais (microcomputadores, smartphones, etc.).
- elasticidade rápida: os recursos computacionais devem ser rapidamenete providos, e rapidamente liberados. O usuário do Serviço de nuvem trabalhará sob a impressão de que possui recursos computacionais ilimitados, que podem ser adquiridos a qualquer momento e em qualquer quantidade.
- serviços mensurados: os sistemas de gerenciamento da nuvem devem fornecer controle e monitoração automática dos recursos computacionais, de modo transparente tanto para o usuário como para o fornecedor do Serviço de nuvem.
- auto-serviço sob demanda: os recursos computacionais são providas de forma automática, sem necessidade de interação humana com o Fornecedor de Nuvem.
- pooling de recursos: os recursos computacionais, sejam físicos ou virtuais, são alocados e realocados conforme a demanda, de modo dinâmico, para servir a múltiplos usuários.

Os modelos canônicos de implementação de nuvem são o de nuvem pública, nuvem privada, e nuvem híbrida. Também existem outros modelos, como o de nuvem comunitária, e o de VPC (Virtual Private Cloud, Nuvem Virtual Privada).

A nuvem pública oferece a infraestrutura de nuvem através do modelo "pague pelo uso", num modelo multi-inquilino. Tais inquilinos são os Clientes de nuvem, entendidos como organizações ou empresas, ao invés de usuários individuais.

A nuvem privada é construída exclusivamente para um único usuário (empresa ou organização). Neste tipo de nuvem, toda a infraestrutura utilizada (servidores físicos e/ou virtuais, links de rede, sistemas de refrigeração, sistemas de alimentação de energia elétrica, etc.) está alocada a um único usuário que, portanto, possui total controle sobre quaisquer implementações a serem feitas nesta nuvem. A modalidade de nuvem privada hospedada em provedor de serviço é possível, mas geralmente uma nuvem privada é construída sobre um datacenter privado.

A nuvem híbrida tem sua infraestrutura resultando da composição de duas ou mais nuvens, que continuam a ser entidades únicas, porém conectadas através de tecnologias que propiciam portabilidade dos dados e/ou aplicações. Tal modelo demanda uma camada adicional de coordenação entre as nuvens que a compõem.

A nuvem comunitária é constituída por uma infraestrutura partilhada por diversas organizações, suportando uma comunidade que possui interesses em comum. Ela pode ser administrada pelas organizações que compõem a comunidade ou por terceiros, e suas instalações podem se situar tanto dentro como fora da comunidade.

Por fim, a VPC (Virtual Private Cloud, ou Nuvem Privada Virtual) pode ser construída sobre infraestrutura de nuvem pública, mantendo muitas das vantagens de uma nuvem

privada, como por exemplo a segregação de recursos computacionais (servidores físicos e/ou virtuais). Por meio da alocação de recursos de rede, serviços de criptografia e de autenticação, é oferecido um certo nível de isolamento entre o usuário da VPC e os demais usuários daquela nuvem pública. Por outro lado, uma VPC pode apresentar necessidades específicas de aprovação por órgãos reguladores para hospedar dados e informações sensíveis.

O quadro-resumo a seguir, baseado na tabela "Cloud Computing Deployment Models" elaborada pela Cloud Security Alliance, apresenta um comparativo de características dos modelos público, privado e híbrido de implantação de computação em nuvem.

Tipo de Nuvem	Infraestrutura gerenciada por	Propriedade da Infraestrutura	Forma de acesso e consumo
Pública	Terceiros	Terceiros	Compartilhado
Privada	Organização e/ou terceiros	Organização e/ou terceiros	Dedicado
Híbrida	Tanto organização como terceiros	Tanto organização como terceiros	Tanto dedicado como compartilhado

Tabela 13. Comparativo dos modelos de implementação de nuvem.

Os modelos canônicos de serviço de nuvem são a IaaS (Infraestrutura como um Serviço), PaaS (Plataforma como um Serviço) e SaaS (Software como um Serviço).

IaaS: serviço que oferece a infraestrutura de processamento e armazenamento de modo transparente, através de mecanismos de virtualização, ainda que não exista o controle sobre os equipamentos físicos, com a possibilidade também de oferecer algum controle, ainda que limitado, sobre os recursos de rede.

PaaS: serviço que oferece para desenvolvedores de aplicativos um modelo de computação, armazenamento e rede, no qual os aplicativos serão executados e disponibilizados.

SaaS: serviço que oferece aplicativos de interesse, hospedando-os na nuvem como alternativa ao processamento local. O acesso a tais aplicativos é feito por meio de navegadores de Internet, e todo o controle e gerenciamento de servidores, armazenamento e rede é feito pelo Fornecedor de Nuvem.

O quadro-resumo a seguir, adaptado a partir da tabela "Exemplos de segmentos e provedores de nuvem pública" elaborada pelo Tribunal de Contas da União, oferece exempos não exaustivos de segmentos de computação disponíveis no modelo de implementação de nuvem pública, e que são oferecidos sob cada modelo canônico de serviço (SaaS, PaaS e IaaS).

Nuvem pública	Segmentos
Software como Serviço (SaaS)	Comunicação e colaboração
	Produtividade de escritório
	Gestão de relacionamento com o cliente (CRM)
	Sistema integrado de gestão empresarial (ERP)
	Supply chain management (SCM)
Plataforma como Serviço (PaaS)	Desenvolvimento de aplicações específicas
	Desenvolvimento de aplicações genéricas
Infraestrutura como Serviço (IaaS)	Computação
	Armazenamento e backup

Tabela 14 - Exemplos de segmentos para cada modelo de serviço de nuvem.

Para Matt Hester's WebLog, conforme adaptação pelo TCU, a divisão de responsabilidades entre cliente e fornecedor de nuvem está representada na figura abaixo:

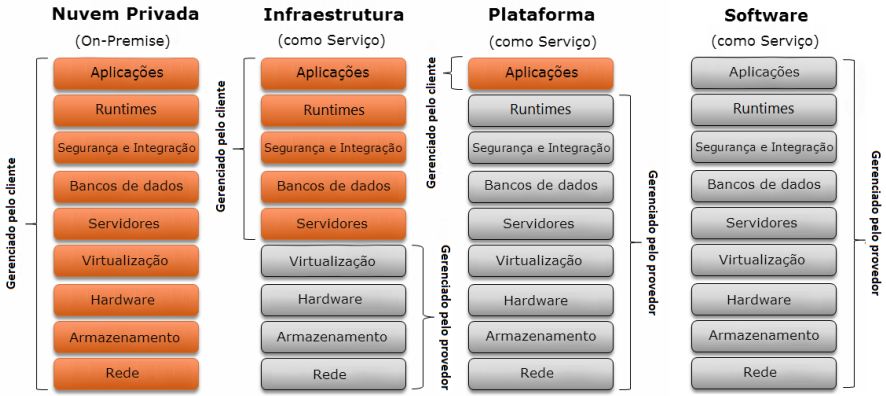


Figura 2 - Divisão de responsabilidades entre cliente e fornecedor de nuvem

A computação em nuvem oferece a oportunidade de reduzir a posse de infraestrutura de tecnologia, por meio do uso de um modelo baseado em consumo de recursos computacionais. Ambientes de computação em nuvem empregam diversas técnicas de virtualização de recursos computacionais (CPU, memória, largura de banda, plataformas, políticas de segurança, dentre outros) para fornecer um meio eficiente de disponibilizar estes recursos no momento em que são necessários, na forma de Serviços de nuvem, abstraindo os recursos computacionais físicos subjacentes. Tal arranjo permite o emprego de um modelo de negócios de pagamento conforme o uso, o que significa que os clientes podem escolher de modo específico quaisquer recursos computacionais que eles precisem, pagando apenas por aquilo que foi efetivamente utilizado. O dimensionamento desses recursos pode, então, ser feito de modo mais categórico, o que é um fator contribuinte para uma possível diminuição de custos.

Os fornecedores de serviços de computação em nuvem adquirem os recursos que compõem a infraestrutura de TIC a um custo menor do que a maior parte das organizações conseguiria, por conta de descontos obtidos com aquisições em volume. Em vários casos, os fornecedores obtêm uma melhor infraestrutura antes que organizações empresariais e governamentais consigam fazê-lo. Abre-se à Administração Pública Municipal a possibilidade de atingir economicidade, por meio de ganho em escalabilidade, em velocidade, ou em ambas.

Por outro lado, a computação em nuvem também pode implicar em custos não previstos ou que não existiam no modelo on premises. Como exemplo, licenças de sofware expiradas, que no modelo on premises podem implicar apenas ausência de suporte técnico, podem (a depender do modelo de hospedagem escolhido) estar a cargo do Fornecedor de nuvem e significar a obrigatoriedade de aquisição de novas licenças, ainda que compartilhando o custo de tais aquisições com os demais inquilinos do Fornecedor de nuvem. Outro exemplo onde pode não ser possível tirar proveito dos ganhos supracitados são aplicações com exigências de arranjos complexos de plataformas computacionais, diferentes das tradicionalmente oferecidas por Fornecedores de nuvem.

BENEFÍCIOS DA COMPUTAÇÃO EM NUVEM

Como possíveis benefícios do uso da computação em nuvem, podem-se citar:

Possibilidade dos investimentos financeiros em TIC passarem da categoria de investimento de aquisição (CAPEX, ou Capital Expenditure) para a categoria de gastos de operação/manutenção (OPEX, ou Operational Expenditure), e da despesa passar a ser distribuída pelos anos em que o Cliente usa a infraestrutura, plataforma ou serviço;

Diminui a obrigatoriedade de imobilização de ativos para investimentos em TIC;

Possibilidade de redução significativa dos custos de TIC;

Aumento da escalabilidade e da flexibilidade no uso dos recursos computacionais;

Possibilidade de aquisição de aplicações mais baratas e fáceis de implementar e usar, na comparação com suas contrapartes on premises.

Possibilidade de contar com suporte técnico adequado e parque tecnológico constantemente atualizado;

Ativos anteriormente imobilizados para TIC podem ser realocados para processos de negócio que sejam críticos para a administração.

Somando-se a estes, podem ser obtidos benefícios adicionais mais específicos para as atividades de TIC de órgãos estatais, a saber:

Maior agilidade na entrega de serviços de TIC e na atualização do parque tecnológico de TIC, dado que os processos burocráticos formais de contratação na administração pública podem dificultar a manutenção de uma infraestrutura de TIC própria que esteja sempre atualizada e à altura das demandas dos usuários;

Para os dados governamentais em sistemas fechados, com função de controle de operações do Estado, e com acesso limitado aos seus operadores, a padronização de equipamentos e software presente em nuvens públicas pode ser mais um elemento facilitador da abertura dessas informações e a consequente ampliação de acesso às mesmas, possivelmente a custo inferior;

Atendimento a picos de demanda sazonal de serviços públicos municipais via Internet, principalmente aqueles com picos próximos a datas limite, ou demandas não sazonais e que gerem picos não previstos de serviço, sem que para tanto seja necessário alocar grande quantidade de recursos fixos;

Aumento da margem de segurança nos procedimentos de controle de contratação de Ativos de TIC, e facilitação da pesquisa de preços, posto que contratações de serviços de nuvem nas modalidades IaaS ou PaaS acontecem por meio de contrato de adesão, com métricas de definição de preços compostas por custos unitários iguais para todos os clientes e disponíveis publicamente. Isso elimina a necessidade das diversas contratações de máquinas, licenças de software, serviços de manutenção e suporte técnico que são necessárias para a operação de infraestrutura de TIC própria;

Velocidade de implantação e economicidade na entrega de serviços de TIC para órgãos com unidades descentralizadas, as quais podem ter a seu dispor o acesso a serviços de TIC por meio da Internet, eliminando a obrigatoriedade de conexões por meio de redes privadas, em geral mais caras.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Em consonância com o Artigo 14 do Decreto Municipal nº 57.653, de 07 de abril de 2017, a contratação de Serviços de Nuvem (bem como de quaisquer outros bens e serviços de TIC) deve estar em conformidade com o PDSTIC do Órgão, bem como com a presente Orientação Técnica.
- Avaliar a existência e disponibilidade de um corpo técnico com quantidade e qualificação adequados para a contratação e gestão dos contratos de computação em nuvem, com suas demandas específicas (por exemplo, de controle e integração dos dados descentralizados, e de segurança da informação)
- Investir em capacitação para ter um corpo técnico adequadamente qualificado para lidar com as questões técnicas relativas à computação em nuvem.
- Garantir junto ao Fornecedor ou Canal de revenda de serviço de nuvem que seus datacenters estejam localizados em países que possuam lei específica de proteção de dados pessoais no mínimo equivalente à Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) - Brasileira. Essa é uma atividade mandatória de acordo com os Art. 5, inciso XV e Art. 33 e 34 da Lei 13.709/2018. Essas informações devem constar claramente nos respectivos contratos.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Ao considerar os benefícios da nuvem, procure levar em conta a questão de escala, considerando se o trabalho adicional que será necessário para a devida configuração técnica e ativação do Serviço de nuvem é justificado por tais benefícios.

PREPARAÇÃO PARA ADOÇÃO DE SERVIÇO DE NUVEM

A etapa de preparação antecede a adoção efetiva de qualquer modalidade de Serviço de computação em nuvem, e tem por objetivo planejar o conjunto de ações que envolve a aquisição de tal Serviço. Os elementos identificados nesta etapa servirão como base para eventual elaboração do edital de contratação do Serviço de nuvem e o respectivo termo de referência.

A preparação é feita por meio de análise prévia de elementos pertinentes à estratégia de TIC do Órgão que pretende adotar o Serviço de nuvem. Independente da abordagem empregada, devem-se ponderar os direcionadores estratégicos e os objetivos de negócio que irão afetar a adoção do Serviço de nuvem, bem como a sua contribuição para a operação e objetivos do negócio.

O profissional responsável pela etapa de preparação, seja ele o detentor do papel de líder de TIC do Órgão, ou servidor da organização por ele delegado, poderá identificar as demandas técnicas e gerenciais a serem atendidas pelo Serviço de nuvem através do apoio do corpo técnico de TIC existente (seja do próprio Órgão, de outros Órgãos que possam exercer papel de apoio técnico, ou oriundo de terceiros) e dos servidores das áreas de negócio.

A elaboração da estratégia de adoção da computação em nuvem é tarefa indelegável a atores externos à organização, em qualquer cenário, sem impedimento da possibilidade de obtenção de apoio técnico por parte de consultorias, fornecedores ou outros agentes externos. Os processos de governança e gestão de TIC de qualquer organização, independentemente do nível de outsourcing das suas atividades de TIC, fazem partem da estratégia de TIC da própria organização.

PLANO DE ADOÇÃO PARA COMPUTAÇÃO EM NUVEM

O plano de adoção para Serviço de nuvem usa os elementos de estratégia identificados durante a preparação. Sua elaboração passa pelas seguintes etapas:

1. Identificar as motivações do Órgão para adoção de Serviço de nuvem, bem como quais modelos de Serviço de nuvem adequam-se às necessidades atuais;
2. Fazer a análise de riscos e decidir, baseado nos riscos identificados, se na situação analisada é aconselhável a adoção de Serviço de nuvem;
3. Tomando como base as necessidades identificadas e a análise dos riscos associados, fazer o levantamento dos modelos de Serviços de nuvem adequados à demanda, bem como dos Fornecedores e modalidades de oferta existentes para tais Serviços;
4. Analisar ainda as possibilidades de armazenamento de dados. Caso os Fornecedores possuam datacenters em outros países, garantir que esses países estão em conformidade com a Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);
5. Elaborar o Edital de contratação e o respectivo Termo de Referência, especificando cláusulas para atender tanto às necessidades e riscos levantados, como também contendo os termos de saída do Serviço de nuvem.

Ao final destas etapas, o Órgão contratante deverá ter subsídios para contratar os fornecedores de serviço de computação em nuvem que estejam alinhados com as demandas e riscos identificadas, e com os termos de saída estipulados.

Os tópicos seguintes desta Orientação Técnica abordarão cada uma das etapas supracitadas.

MOTIVAÇÕES PARA ADOÇÃO DE COMPUTAÇÃO EM NUVEM

A computação em nuvem traz a possibilidade de uma série de benefícios. Ainda assim, nem tudo pode ou deve necessariamente ir para a nuvem.

Em termos práticos, cargas de trabalho com projeção de crescimento apenas vegetativo podem não obter benefícios de economicidade com a mudança para computação em nuvem.

Outra possível limitação apresenta-se para cargas de trabalho que tenham que permanecer hospedadas em servidores locais, devido a obrigatoriedade de aderência a regulamentos/legislações, ou devido a outro vínculo forte com local físico, ou ainda a regulamentos/legislações dos países nos quais os dados ficarão hospedados e que possam interferir na privacidade dos dados.

Um dos fatores empregados para verificar se determinado modelo de computação em nuvem adequa-se à demanda é levar em conta a competitividade em termos de custo tanto no momento presente, como em curto prazo (dali a três anos, por exemplo).

Após identificar as motivações para adoção de Serviço de nuvem, a etapa seguinte é verificar qual modelo de serviço de nuvem melhor se ajusta ao caso, decidindo entre IaaS, PaaS, SaaS, ou outros modelos derivados destes.

ANÁLISE DE RISCOS

A adoção da computação em nuvem, ou de qualquer outro modelo computacional, envolve riscos para os Ativos de Informação envolvidos e, consequentemente, para os negócios da Administração Municipal.

Por conta disso, a escolha e consequente investimento na computação em nuvem devem ser guiados pela análise dos

benefícios que serão obtidos pelo seu uso, porém dentro de um nível de risco que seja aceitável pela Administração.

Após levantar as motivações para adoção de Serviço de nuvem, e o modelo de Serviço de nuvem que deverá atender as necessidades identificadas, a etapa seguinte é a análise a criticidade dos Ativos de Informação para a Administração Municipal.

A análise dos elementos de criticidade de tais Ativos, em conjunto com a avaliação do valor gerado pelo emprego de Serviço de nuvem, fornecerá elementos para desenhar os critérios de decisão da adoção ou não do Serviço de nuvem.

Como boa prática, a avaliação de criticidade e a determinação do Valor do Ativo podem ser uma tarefa desempenhada em conjunto entre o corpo técnico de TIC e os servidores da área de negócio do Órgão.

QUADRO-RESUMO

O quadro-resumo a seguir oferece elementos de apoio para decisão de adoção ou não de Serviço de Nuvem, a partir da classificação de criticidade dos Ativos de Informação, associado ao valor percebido do uso do Serviço de Nuvem para a Administração Municipal.

Criticidade do Ativo de Informação	Valor gerado para a Administração Municipal	Usar nuvem?
Baixa	Alto/Médio/Baixo	Sem restrições
Média	Alto	Benefício for maior que os riscos.
Média	Médio	Alto risco, e valor incerto.
Média	Baixo	Alto risco, e valor incerto.
Alta	Baixo	Alto risco, e valor incerto.
Alta	Alto	Se o benefício for maior que os riscos.
Alta	Médio	Alto risco, e valor incerto.
Alta	Baixo	Desaconselhada em qualquer cenário.

Tabela 17: Risco do uso de nuvem a partir de criticidade dos ativos de TIC envolvidos.

No quadro-resumo, foram empregadas as seguintes categorias de classificação para a contratação de computação em nuvem:

- contratação sem restrições;
- contratação liberada caso o benefício aos negócios seja maior que os riscos;
- contratação de alto risco e valor incerto para os negócios;
- contratação desaconselhada em qualquer cenário.

De modo geral, quando o valor que espera-se gerar para os negócios da Administração Municipal com a adoção de um Serviço de nuvem for baixo, e ao mesmo tempo a criticidade do Ativo de Informação envolvido for alta, entende-se que a adoção de tal Serviço de nuvem seja desaconselhada. Já no caso da criticidade do Ativo de Informação ser baixa, não há restrições para a contratação de Serviço de nuvem.

Caso decida-se pela adoção de Serviço de nuvem, deve-se estabelecer os riscos gerados para a Administração Municipal, as formas pelas quais tais riscos serão mitigados, e o estabelecimento de sistemas e registros de monitoração e controle desses riscos. Tais elementos guiarão a escolha do Serviço de nuvem específico a ser adotado, dentro de níveis de risco considerados aceitáveis pela Administração.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Realizar as análises e avaliações pertinentes para o Plano de adoção para computação em nuvem, conforme disposto nesta Orientação Técnica.
- Avaliar as questões técnicas de integração das redes computacionais da Prefeitura do Município de São Paulo com a rede do Fornecedor de Nuvem, levando em conta o uso de boas práticas de segurança da informação como, por exemplo, endereços IPs privados dentro da nuvem e IPs

públicos fora dela, estabelecimento de regras adequadas de firewall, estabecimento da segurança das portas de rede que ficarão expostas à rede pública no caso de aplicativos acessíveis aos munícipes e, no caso de aplicativos internos à Prefeitura, a escolha de intranet ou internet, VPN site-to-site, alocação de intervalo de endereços IP para a VPC (Virtual Private Cloud), definição de pontos de segurança por meio do firewall, inserção de pontos de controle no firewall da PMSP bem como no do Fornecedor de nuvem, sem prejuízo de outras boas práticas.

QUAIS SÃO AS NOSSAS SUGESTÕES?

Para guiar a elaboração de uma estratégia de adoção de computação em nuvem, pode-se buscar respostas para as seguintes perguntas:

- Existe um plano de adoção para a computação em nuvem?
- O plano de adoção da computação em nuvem está conforme estabelecido em seu PDSTIC, bem como alinhado com o PETIC da Administração Municipal, se houver uma disposição nesse sentido no PETIC?
- Existe uma avaliação de custos e benefícios?
- Existe uma avaliação do nível de maturidade do órgão/setorial/secretaria para a adoção da computação em nuvem?
- Foi levado em conta o investimento que já foi realizado e será perdido a partir da adoção da computação em nuvem?
- Existe estratégia para medir de modo objetivo se os benefícios planejados estão sendo alcançados?
- Existe um levantamento e avaliação dos riscos?
- Existe um plano de gerenciamento dos riscos?
- Quais capacidades de gestão deverão ser desenvolvidas ou adquiridas para cuidar da computação em nuvem?

- Existe uma avaliação sobre como as informações do Órgão estão garantidas e protegidas na nuvem?

Para elaborar o plano de adoção para um Serviço de nuvem, as seguintes etapas podem servir como balizamento:

- Listar os Ativos de Informação a serem migrados para a nuvem, definir o Valor do Ativo de cada um deles, e a partir destas informações, classificá-los em níveis crescentes de criticidade;
- Classificar o valor para os negócios que espera-se que a contratação de Serviço de nuvem e/ou migração para a nuvem deva gerar para a Administração Municipal;
- Avaliar os riscos inerentes à computação em nuvem, em seus aspectos técnicos, jurídicos, organizacionais e comuns;
- Cruzar as informações de criticidade, de valor para os negócios, e a avaliação de riscos, para informar se a contratação do Serviço de nuvem é liberada em qualquer cenário, se depende dos benefícios gerados, ou se é desaconselhada em qualquer cenário, e assim embasar a decisão de oportunidade ou não da contratação do Serviço de nuvem;
- Avaliar também o risco do fim do ciclo de vida de seu produto, bem como de cláusulas de obsolescência programada (por exemplo, oferta de suporte técnico limitada à versão atual e a imediatamente anterior do produto), e buscar iniciar as negociações de renovação com antecedência suficiente para, caso necessário, permitir a migração para outro fornecedor e/ou tecnologia.

OPÇÕES DE SERVIÇOS DE NUVEM

Após concluir a preparação para adoção de computação em nuvem, a etapa seguinte é efetuar o levantamento das opções disponíveis de Serviços de nuvem, e dos respectivos Fornecedores de nuvem que proverão tais Serviços, visando escolher a opção mais adequada dentro dos elementos de estratégia identificados e do plano de adoção elaborado.

FORNECEDORES DE NUVEM

Tomando por base os modelos canônicos de serviço de nuvem (IaaS, PaaS e SaaS), o mercado de nuvem no Brasil apresenta-se, de modo geral, dividido conforme segue.

- Fornecedores no modelo IaaS: dentro da modalidade de Infraestrutura como um Serviço, pode-se identificar quatro grandes grupos de Fornecedores:
  - empresas multinacionais;
  - empresas regionais ou de nichos específicos;
  - empresas de telecomunicações que oferecem serviços de terceirização para a nuvem;
  - empresas locais.
- Fornecedores no modelo PaaS: na modalidade de Plataforma como um Serviço, pode-se encontrar, por exemplo, Fornecedores de:
  - plataforma para desenvolvimento de aplicações;
  - infraestrutura para execução de aplicações;
  - soluções de BI (Business Intelligence, ou Inteligência de Negócios);
  - soluções de bancos de dados.
- Fornecedores no modelo SaaS: na modalidade de Software como um Serviço, é possível identificar, por exemplo, Fornecedores de:
  - Aplicações de CRM (Customer Relationship Management) e ERP (Enterprise Resource Planning);
  - Atendimento a pequenas empresas, com fornecimento de suítes de escritório e de aplicações, como sistemas de contabilidade;

INTEGRADORES DE NUVEM

O aumento no uso de serviços de nuvem criou no mercado consumidor a expectativa que os Fornecedores de nuvem ofereçam serviços profissionais de consultoria e suporte para auxiliá-los na transição do modelo computacional tradicional para o modelo de computação em nuvem. Além disso, o mesmo aumento também criou pressão para que as empresas de telecomunicações, de hospedagem de serviços e integradoras de sistemas passem a oferecer um leque cada vez maior de serviços de TIC por meio de nuvem.

Em atendimento a tais demandas, surgiu o serviço de Integração de Serviços de Nuvem (Cloud Service Brokerage), bem como o respectivo papel de Integrador de Nuvem (Cloud Broker).

O Integrador de Nuvem é uma empresa que age como intermediária entre o Cliente e o Fornecedor de Nuvem. Seu objetivo final é o de orientar seus clientes na escolha do Serviço de Nuvem mais adequado, facilitando o processo durante as negociações por meio de ações consultivas, conhecimento de mercado e relacionamento já estabelecido com Fornecedores de Nuvem, obviamente a um custo adicional agregado. O Integrador de Nuvem, portanto, desempenha um papel que vai além daquele exercido pelos Canais de Revenda.

Conforme aumenta o uso de soluções de computação em nuvem, e consequentemente diminuem os recursos próprios de TIC dentro das organizações, existe a tendência de que os profissionais de TIC das organizações passem a desempenhar o papel de Integrador de Nuvem, orientando as áreas de negócio na contratação dos serviços de nuvem adequados.

PRECIFICAÇÃO DE NUVEM

A existência das diversas formas sob as quais a computação em nuvem apresenta-se, tanto em termos de modelos de implantação e modelos de serviço, como dos modos pelos quais tais modelos são oferecidos pelos Fornecedores de nuvem, fazem com que não seja trivial a tarefa de estabelecer uma comparação entre Fornecedores de nuvem, ou mesmo de estabelecer parâmetros de avaliação dos modelos de comercialização de Serviços de nuvem existentes.

O modelo de pagamento geralmente adotado é o de pagamento por uso dos recursos, ainda que existam mecanismos de cobrança por usuário quando da contratação de Software como um Serviço. No entanto, dada a natureza dinâmica deste mercado, muitos Fornecedores de nuvem oferecem combinações complexas de uso de diversos recursos computacionais, e o Cliente terá que envidar esforços para encontrar uma combinação que forneça a melhor relação de custo-benefício.

A comparação entre Fornecedores de Nuvem baseia-se numa análise do Custo Total de Propriedade (ou TCO, Total Cost Ownership), em conjunto com características de flexibilidade, atendimento e recursos disponibilizados. Para fins de ilustração, segue abaixo uma lista de variáveis que podem ser consideradas na comparação entre os diferentes Fornecedores de Nuvem.

1. Precificação;
2. Preço mensal médio;
3. SLA de disponibilidade;
4. Quantidade de datacenters;
5. Capacidade de ampliação (scale up, ou capacidade de ampliar individualmente as instâncias de equipamentos servidores, por meio da adição de CPU, memória ou armazenamento);

6. Capacidade de crescimento (scale out, ou capacidade de implantar novas instâncias de equipamentos servidores);
7. Suporte técnico;
8. Monitoramento e alerta;
9. Existência de período de gratuidade para teste;
10. Existência de APIs como interfaces para interação com os servidores;
11. Número de tipos diferentes de sistemas operacionais suportados;
12. Número de tipos de instâncias de servidores;
13. Custo de saída de dados;
14. Custo de entrada de dados.

Tais variáveis, ainda que mais facilmente identificadas com o segmento de Fornecedores de nuvem na modalidade Infraestrutura como Serviço, e apesar de representarem uma pequena fração dentre todas as variáveis de comparação possíveis, estabelecem parâmetros mínimos para fins de comparação ou, ao menos, para serem observados quando da contratação.

FÓRMULAS DE PRECIFICAÇÃO

A seguir, são apresentadas fórmulas para o cálculo de custo dos Serviços de Nuvem, dentro dos modelos canônicos de serviço (IaaS, PaaS e SaaS).

Em que pese os preços de Serviços de Nuvem serem resultado direto da combinação entre Custo Total de Propriedade (ou TCO, Total Cost Ownership), e características de flexibilidade, atendimento e recursos disponibilizados, as fórmulas aqui apresentadas oferecem elementos básicos relacionados à precificação, com objetivo de embasar análise das componentes de preço apresentadas por Fornecedores de nuvem,

e podem ser adaptadas para adequarem-se aos diversos contextos em que forem necessárias.

Sob o modelo de Infraestrutura como um Serviço, uma fórmula básica pode considerar o seguinte:

IaaS = horas de computação + horas de armazenamento + custos de software

Para o modelo de Plataforma como um Serviço, por possuir muitas variáveis de custo, pode-se considerar uma fórmula mais simplificada, como por exemplo:

PaaS = horas de armazenamento + (nº de chamadas API * preço por chamada API) + duração de consultas

Já no modelo de Software como um Serviço, a precificação geralmente baseia-se em quantidade de usuários, e volume e tipo dos recursos consumidos, ou uma combinação destes. (Uma analogia possível é a cobrança por consumo de água ou energia elétrica.)

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Uma vez decidido que será contratado Serviço de computação em nuvem, avaliar as variáveis relevantes para a análise dos Fornecedores de Nuvem, inclusive caso haja restrições relacionadas aos países onde os servidores serão alocados, se eles têm uma política de proteção de dados pessoais no mínimo equivalente à 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);
- Utilizar ou desenvolver uma ou mais formas de precificação para o cálculo de custo dos Serviços de Nuvem, para se ter as estimativas adequadas do investimento a ser realizado.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Na avaliação de Fornecedores de nuvem sob o modelo de Plataforma como um Serviço (PaaS), caso os mesmos usem ferramentas que são padrão de mercado a comparação direta das ferramentas oferecidas (linguagens de programação, sistemas de bancos de dados, etc.) pode não ser útil. Nesse caso, procure avaliar outros itens que indiquem o grau de controle do Fornecedor sobre a infraestrutura que sustenta a plataforma, tais como:
  - suporte oferecido durante o ciclo de vida de desenvolvimento da aplicação;
  - serviços de versionamento, testes e implantação da aplicação em produção (deploy);
  - APIs oferecidas;
  - gerenciamento de logs;
  - feedback.

- Abordar a questão de como estabelecer cobrança para inovações tecnológicas na nuvem. Por exemplo, novas features que não existiam no momento da contratação e que aumentem a flexibilidade da nuvem podem incorrer em novos custos, e são portanto um ponto de atenção, especialmente para os Serviços de Nuvem contratados sob modelo de Plataforma como Serviço (PaaS). O apoio jurídico para construção de solução a este respeito pode ser relevante.

ELABORAÇÃO DO EDITAL E TERMO DE REFERÊNCIA

A última fase da elaboração de um plano de adoção de Serviço de Nuvem é a elaboração do edital e termo de referência para a contratação do Fornecedor de Nuvem.

Durante esta fase, é importante dedicar mais tempo às cláusulas que sejam mais importantes e que tenham maior probabilidade de interfer diretamente e de modo importante no uso dos Serviços de nuvem, e na maneira pela qual o Fornecedor de Nuvem provê tais Serviços.

Para tal efeito, é possível organizar as cláusulas do edital e termo de referência de acordo com o grau de importância que assumem. Assim, será possível direcionar maior foco à elaboração das cláusulas que têm maior impacto sobre o resultado final da contratação.

CLASSIFICAÇÃO DAS CLÁUSULAS POR GRAU DE IMPORTÂNCIA

De acordo com seu grau de influência no resultado final do Serviço de Nuvem, as cláusulas contratuais podem ser categorizadas em cláusulas críticas, importantes, e interessantes.

Por sua natureza de Orientação Técnica, este documento foca em cláusulas relacionadas aos aspectos técnicos do Serviço de Nuvem. Tais exemplos não pretendem exaurir todas as possibilidades existentes, e os Órgãos contratantes são encorajados a acrescentarem cláusulas que entendam importantes para atingir seus objetivos com a contratação do Serviço de Nuvem, sem prejuízo das demais cláusulas que abordem outros aspectos da contratação.

A seguir, são apresentadas as definições de cada uma destas categorias.

Das cláusulas críticas

As cláusulas críticas para contratação de Fornecedor de nuvem tratam de tópicos que têm alta probabilidade de ocorrência, que incorram em alto risco para a execução do serviço e continuidade dos negócios, e/ou que tenham forte influência no caso de decisão de saída da nuvem.

São críticas as cláusulas que dispõem sobre:

- encerramento do serviço;
- segurança dos dados, processos e/ou serviços;
- proteção à privacidade dos dados, processos e/ou serviços.

Das cláusulas importantes

As cláusulas importantes para contratação de Fornecedor de nuvem tratam de tópicos que incorrem em algum risco para a execuçao do Serviço de nuvem e continuidade dos negócios, mesmo aquelas com baixa probabilidade de ocorrência, além de poderem influenciar no caso de decisão de saída da nuvem. São importantes as cláusulas que dispõem sobre:

- monitoramento do atendimento ao SLA acordado;
- soberania dos dados;
- uso de subcontratação;
- não responsabilização e indenização;
- encargos de reaquisição de dados;
- auxílio pós-término do contrato;
- confidencialidade.

Das cláusulas interessantes

As cláusulas interessantes para contratação de Fornecedor de nuvem tratam de tópicos que, ainda que tragam interesse para o Cliente, não definem o comportamento dos Fornecedores de nuvem. São cláusulas interessantes aquelas que dispõem sobre:

- portal de administração da nuvem;
- notificação global;
- programas de desconto;
- serviços não decrescentes;
- créditos de serviços;
- definição dos conceitos presentes no SLA;
- definição de força maior.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- É mandatório para qualquer contratação de nuvem a existência, no edital, de garantias mínimas com relação às cláusulas críticas;
- Com respeito às Cláusulas Críticas, considere os seguintes exemplos:
  - Cláusulas de encerramento do serviço:
    - Prever que o Fornecedor ofereça à Contratante, após o fim do contrato de serviços e por um período razoável de tempo, a capacidade de readquirir/exportar os dados (e código-fonte, no caso de PaaS ou IaaS), na forma em que estes se encontravam à época do final do contrato, e com custos definidos pela tabela de preços do Fornecedor vigente à época.
    - Prever que, após este período e somente após este período, Fornecedor deletará, inutilizará ou de outra maneira tornará inacessíveis os dados que ainda estejam em suas dependências ou sob sua responsabilidade.
    - Prever os formatos de dados específicos que serão empregados para exportação dos dados ao final do contrato, preferencialmente formatos abertos e/ou padronizados;
  - Cláusulas de segurança:
    - Prever que o Fornecedor implemente medidas e recursos razoáveis e apropriados com o objetivo de auxiliar a Contratante a proteger seus dados contra os eventos de perda, acesso ou divulgação, sejam estes eventos acidentais ou ilegais.

 Prever garantias por parte do Fornecedor com relação à disponibilidade, integridade, confidencialidade e autenticidade das informações hospedadas na nuvem, em especial das informações sob custódia e gerenciamento pelo Fornecedor.

 Prever que o ambiente de serviço do Fornecedor de nuvem esteja em conformidade com a norma ABNT NBR ISO/IEC 27002:2013, sem prejuízo de outras exigências.

 Prever que o Fornecedor aloque auditores terceiros, para que estes realizem o exame dos sistemas e serviços de acordo com as recomendações de melhores práticas presentes em quadros de trabalho de compliance como o ABNT NBR ISO/IEC 27002:2013, e/ou em padrões de indústria equivalentes.

 Prever também que o Fornecedor forneça sob demanda da Contratante os relatórios resultantes destes exames de auditoria, como por exemplo os relatórios do tipo SOC (Controle de Organização de Serviço), e que a periodicidade de elaboração de tais relatórios esteja pré-definida.

 Prever a possiblidade de que a Contratante ou seus representantes possam realizar, às próprias custas e desde que não estejam já inclusas nos exames de auditores independentes em vigor, revisões físicas e/ou eletrônicas da segurança do sistema/serviços hospedados no Fornecedor, ou avaliações e monitoramento do nível de compliance do Fornecedor com relação às obrigações de segurança estipuladas no contrato.

■ Cláusulas de proteção à privacidade:

 Prever a possibilidade ou impossibilidade de o Fornecedor transferir os dados da jurisdição onde encontra-se a Contratante para outra, seja dentro ou fora do Brasil, tendo em mente que os responsáveis pelos dados nestas novas jurisdições podem estar sujeitos à legislações de privacidade menos abrangentes ou não equivalentes àquelas vigentes na jurisdição original.

 O Fornecedor deverá ter implementado uma política interna de proteção aos dados pessoais que preveja quais medidas devem ser adotadas em caso de vazamento de informações.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Com respeito às Cláusulas Importantes, considere os seguintes exemplos:
  - Cláusulas de monitoramento do atendimento ao SLA:
    - Prever que a Contratante tenha direito a auditar os registros de atividade (logs) de desempenho do Fornecedor, e que tenha acesso às estatísticas de qualidade do serviço, bem como estipular se o monitoramento, no nível de detalhe desejado, incorrerá em custos.
  - Cláusulas de soberania dos dados:
    - Prever que os dados e informações do Cliente residam exclusivamente em território nacional, incluindo dados de replicação e cópias de segurança (backup), de forma que o Cliente esteja amparado pela legislação brasileira.
    - Prever que seja adotado o foro brasileiro para dirimir quaisquer questões jurídicas relacionadas ao contrato firmado entre o Fornecedor de nuvem e o Cliente.
  - Cláusulas de uso de subcontratação:
    - Prever, no caso da existência do Canal de Revenda, se a aceitação das cláusulas contratuais será feita pelo Canal de Revenda ou diretamente pelo Fornecedor de Nuvem.
    - Prever, nos casos de nuvem sob os modelos de Infraestrutura como Serviço (IaaS) ou Plataforma como Serviço (PaaS) e que sejam gerenciadas pela revenda, a responsabilização pela qualificação técnica mínima dos profissionais.
    - Prever veto de acesso aos dados e/ou processos por parte da Revenda, para aqueles serviços de nuvem não gerenciados por ela.
    - Prever, caso necessário, garantias explícitas de que não existam terceiros envolvidos na execução das obrigações do Fornecedor estipuladas no contrato, e/ou que nenhuma empresa subcontratada ou terceira acesse os dados da Contratante, salvo sob expressa autorização desta.
    - Prever a possibilidade ou impossibilidade de que o

Fornecedor retenha os dados da Contratante para fins de negócios do próprio Fornecedor, e que estes dados estejam acessíveis aos empregados do Fornecedor em relação a este fim, e que sejam retidos e/ou processados por terceiros que forneçam serviços ao próprio Fornecedor.

■ Cláusulas de não responsabilização e de indenização:

 Prever contextos e limites para a não responsabilização e para indenizações que visem proteger o Fornecedor, no caso de terceiros levantarem alegações contra o Fornecedor relacionados aos dados do Cliente, ao uso que a Contratante faz dos serviços de nuvem do Fornecedor, ou de violações dos termos destes serviços por parte da Contratante.

 Prever indenizações entre as partes contra alegações de violação de propriedade intelectual de terceiros ocorridas a partir dos serviços de nuvem, e de possíveis reclamações, responsabilizações, danos, perdas e despesas oriundas destas violações.

 Prever que o Fornecedor ofereça notificação escrita no caso de tais alegações, bem como forneça assistência razoável, às custas do Fornecedor.

■ Cláusulas de encargos de reaquisição dos dados:

 Prever que o Serviço de nuvem a ser contratado permita a portabilidade de dados e aplicativos e que as informações do órgão contratante estejam disponíveis para transferência de localização, em prazo adequado e sem custo adicional, de modo a garantir a continuidade do negócio e possibilitar a transição contratual.

■ Cláusulas de auxílio pós-término do contrato:

 Prever que, quando do encerramento do contrato, o Fornecedor ofereça suporte logístico, técnico e operacional durante período adequado de tempo e com custos pré-definidos pela tabela de preços do Fornecedor vigente à época do contrato, com objetivo de viabilizar e apoiar o processo de reaquisição dos dados, processos e/ou serviços de TIC e assim garantir a continuidade do negócio e possibilitar a transição contratual.

- Cláusulas de proteção à confidencialidade:
  - Prever que o Fornecedor não revele dados do Cliente em nenhuma hipótese, exceto se exigido pelos órgãos legais competentes, e que, na ocorrência de tal exigência por órgãos legais, o Fornecedor envide esforços para direcionar a exigência diretamente para a Contratante. Caso tal direcionamento não seja possível, prever que o Fornecedor prontamente apresente à Contratante cópia da demanda, a menos que seja impedido de fazê-lo por determinação de órgão legal competente.

Com respeito às Cláusulas Interessantes, considere os seguintes exemplos:

- Cláusulas sobre portal de administração da nuvem
  - Prever, no caso de existir um Canal de Revenda, se este deverá ter acesso ao Portal de administração da nuvem.
  - Prever se será possível ativar serviços que estejam fora do escopo do Termo de Referência por meio de autocomissionamento feito diretamente pela Contratante, sem intervenção do Fornecedor ou Canal de Revenda, e como tal situação deverá ser faturada.
  - Prever se o fiscal de contrato será o único com acesso ao Portal de administração e, desse modo, se exercerá de modo exclusivo a função de controle do contrato.

- Cláusulas sobre notificação global
  - Prever a existência de uma política de notificação global por parte do Fornecedor de nuvem, que informe contatos da Contratante no evento de uma alteração de status de um host, de um serviço, ou de um serviço de usuário.
  - Prever os mecanismos de tal política de notificação global, como por exemplo: slots de tempo para notificação, lista de contatos da Contratante a serem notificados, e qual a política de notificação para cada host individual, para cada serviço individual, e para cada serviço de usuário individual.

- Cláusulas de créditos de serviços
  - Prever a ocorrência de créditos de serviço em favor da

Contratante para situações onde o Fornecedor não consiga cumprir o índice de disponibilidade de serviço. Por exemplo:

- Disponiblidade mensal abaixo de 99,95% gera um crédito de serviço de 10% sobre o valor total mensal;
- Disponiblidade mensal abaixo de 99% gera um crédito de serviço de 25% sobre o valor total mensal;
- Disponiblidade mensal abaixo de 95% gera um crédito de serviço de 50% sobre o valor total mensal.

- Cláusulas de definição dos conceitos presentes no SLA

 Prever o estabelecimento de definições claras para o amplo leque de terminologia empregada pelo Fornecedor de Nuvem, uma vez que cada Fornecedor emprega termos próprios e não existe padrão ou uniformidade entre eles. Para citar um exemplo, no tópico de disponibilidade, são encontrados nos SLAs de diferentes fornecedores termos como "máximo de minutos disponíveis", "tempo de inatividade" e "porcentagem de tempo de atividade mensal" para um deles, e "inatividade" e "porcentagem de atividade mensal" para outro, e dentro de tais conceitos o cálculo de preços pode variar.

- Cláusulas de força maior

 Prever os limites de responsabilização do Fornecedor por conta de falhas ou interrupção do Serviço de nuvem, causadas direta ou indiretamente por uma força maior que esteja além do controle razoável do Fornecedor.

 Prever que tais limites de responsabilização dependem de a parte em não cumprimento notificar prontamente a outra parte, e tomar todas as providências razoáveis para voltar a cumprir suas obrigações tão logo quanto possível.

 A título de exemplo, uma situação de força maior pode ser causada por: razões técnicas (como vírus de computador, ciberataques, falhas na Internet, nas telecomunicações ou em qualquer outro equipamento, e falhas no fornecimento de energia elétrica); atos da natureza (como incêndios, enchentes, tempestades e furacões); itens relacioados à comunidade onde o Fornecedor está inserido (como pandemias, greves, distúrbios civis, tumultos e inssurreições);

e outros itens diversos (como falta de mão de obra, falta de materiais, guerras, explosões, terrorismo, ações governamentais, ordens judiciais nacionais ou estrangeiras, bem como não cumprimento de terceiros).

- Somando-se às motivações levantadas durante a etapa de preparação para adoção de Serviço de nuvem, é importante considerar os seguintes tópicos no momento da escolha do Fornecedor de nuvem:
  1. Preparação para resposta a incidentes;
  2. Existência de cobrança mensal conforme o uso dos recursos;
  3. Existência de suporte técnico;
  4. Custo inicial baixo;
  5. Experiência técnica.

- Na elaboração do SLA a ser seguido pelo Fornecedor de nuvem escolhido, é interessante que os seguintes tópicos estejam previstos:
  1. Existência de serviço alternativo em caso de incidente crítico;
  2. Tempo mínimo de serviço no ar;
  3. Tempo médio de recuperação de falhas;
  4. Tempo médio de resposta;
  5. Disponibilidade do serviço (em % sobre o tempo total considerado);
  6. Total de horas do serviço (incluindo help desk, dentre outros);
  7. Metodologia dos backups;
  8. Período de retenção dos backups;
  9. Capacidades de registro de atividades (log);
  10. Processo de reporte de falhas.

REFERÊNCIAS

REFERÊNCIAS LEGAIS:

Brasil. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal, e dá outras providências. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a transferência internacional de dados no inciso XV do art. 5º, nos art. 33 a 36 da Constituição Federal, e dá outras providências. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2015-2 18/2018/lei/l13709.htm>.

Brasil. Norma Complementar 14/IN01/DSIC/GSIPR – Diretrizes relacionadas à segurança da informação para o uso de computação em nuvem nos órgãos e entidades da Administração Pública Federal. Disponível em <http://dsic.planalto.gov.br/legislacao/nc_14_nuvem.pdf>.

Brasil. Ministério do Planejamento, Orçamento e Gestão. Boas práticas, orientações e vedações para contratação de Serviços de Computação em Nuvem. Disponível em <https://www.governoeletronico.gov.br/documentos-e-arquivos/Orientacao%20servicos%20em%20nuvem.pdf>.

Tribunal de Contas da União. Acórdão 1739, Processo 025.994/2014-0. Disponível em <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20150720/AC_1739_24_15_P.doc>.

REFERÊNCIAS BIBLIOGRÁFICAS:

ABREU, Vladimir Ferraz de; FERNANDES, Aguinaldo Aragon. Implantando a governança de TI: Da estratégia à Gestão de Processos e Serviços. 4a edição. Rio de Janeiro: Brasport, 2014.

BARROS, Daniel. Contract Negotiation Clinic: IaaS and PaaS. Gartner Symposium ITXPO, 23-26 out. 2017.

BRASIL. GOVERNO DIGITAL. Guia de boas práticas Lei Geral de Proteção de Dados (LGPD). Abr. 2020. Disponível em: <https://www.gov.br/governodigital/ptbr/ seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf >. Acesso em: 25 mar. 2022. p. 12.

BRASIL. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 25 mar. 2022.

Configuring Notifications. Coservit ServiceNav. Website, disponível em <http://servicenav.coservit.com/documentation/configuring-notifications/>. Último acesso em 20 out. 2017.

Cloud Security Alliance. Security Guidance for critical areas of focus in cloud computing v3.0. EUA: Cloud Security Alliance, 2011. Disponível em <https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf>. Necessário cadastro prévio. Último acesso em 20 out. 2017.

FERNANDES, D.A.B.; SOARES, L.F.B.; GOMES, J.V. et al. Security issues in cloud environments: a survey. In International Journal of Information Securiry (2014) 13: 113. Disponível em <https://doi.org/10.1007/s10207-013-0208-7>. Último acesso em 20 out. 2017.

HOGBEN, Giles. Privacy, Security and Identity in the Cloud. Comunidade Europeia: European Union Agency for Network and Information Security, 2010. Disponível em <https://www.enisa.europa.eu/topics/cloud-and-big-data/Cloud_Identity_Hogben.pdf>. Último acesso em 20 out. 2017.

HARADA, Yonosuke. Study on Cloud security in Japan. Japão: ITGI, 2011. Disponível em <http://m.isaca.org/Knowledge-Center/Research/Documents/Study-on-Cloud-Security-in-Japan_res_Eng_0211.pdf>. Último acesso em 20 out. 2017.

IMONIAMA, Joshua. Seminário de Cloud Computing. FEA/USP. Disponível em <https://edisciplinas.usp.br/mod/resource/view.php?id=1194478>. Último acesso em 16 jan. 2018.

MELL, Peter; GRANCE, Timothy. The NIST Definition of Cloud Computing: Special Publication 800-145. EUA: National Institute of Standards and Technology, 2011.

VERAS, Manoel. Computação em Nuvem: Nova Arquitetura de TI. Rio de Janeiro: Brasport, 2015.

[OT 010]
CRITÉRIOS GERAIS DE GESTÃO DE APLICAÇÕES

98 ESCOPO E CONTEXTO

98 DEFINIÇÕES

100 CONTRATAÇÃO, ALUGUEL, ADOÇÃO OU DESENVOLVIMENTO

103 RACIONALIZAÇÃO E CONSOLIDAÇÃO

107 PADRONIZAÇÃO DE APLICAÇÕES

109 REFERÊNCIAS

Visa orientar os servidores definindo diretrizes na gestão de aplicações contendo inicialmente disposições gerais a respeito dos modelos de aquisição de uma aplicação e o benefício de cada modalidade seja contratação, aluguel, adoção ou desenvolvimento. Define então a racionalização e consolidação de uma ou mais aplicações considerando o valor no negócio, a eficiência e a segurança tecnológicas com a finalidade de padronizar o processo de adoção de uma aplicação.

ESCOPO E CONTEXTO

Fazem parte do escopo desse documento as diretrizes gerais a respeito da gestão de aplicações.

As diretrizes específicas serão dispostas em Orientações Técnicas posteriores, sem prejuízo da revisão desta Orientação.

Não fazem parte do escopo desta OT as metodologias de desenvolvimento de aplicações, tampouco os processos administrativos para a contratação de aplicações ou de seu desenvolvimento.

DEFINIÇÕES

Os modelos de aquisição de uma aplicação são: Contratação, Aluguel, Adoção ou Desenvolvimento.

Contratação é a aquisição de uma aplicação proprietária, customizável ou não, desenvolvida por um ou mais fornecedores externos, seja por meio de licenças de uso ou de subscrição/assinatura.

Aluguel é a aquisição de uma aplicação disponível como serviço (SaaS – Software as a Service), customizável ou não, desenvolvida por terceiros.

Adoção é a utilização de uma aplicação disponível como software de código livre ou código aberto, customizável ou não, desenvolvida por terceiros.

Desenvolvimento é a construção de uma aplicação, seja utilizando mão-de-obra interna, seja contratando os serviços do Integrador Estratégico ou ainda de um ou mais fornecedores externos.

Doação é apenas uma forma de obtenção de software que poderá estar relacionada com os itens Contratação,Aluguel e Desenvolvimento.

Independentemente do modelo de aquisição da aplicação, esta deverá estar prevista no respectivo PDSTIC do Órgão Setorial.

O Órgão Central poderá definir padrões, metodologias e aspectos técnicos a serem adotados por todos os Órgãos Setoriais, mediante prévia divulgação no Portal de Governança.

Os ambientes de teste/homologação deverão estar apartados do ambiente de produção.

O Órgão Setorial poderá, a seu critério, separar os ambientes de teste e de homologação.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Contemplar os requisitos de infraestrutura e de segurança da informação quando da aquisição de uma aplicação.
- Evitar a realização de Testes em ambiente de produção, que deverão ser realizados em ambiente de teste/homologação. Entretanto, excepcionalmente, e para resolução de incidentes graves, testes poderão ser feitos de maneira pontual e por prazo limitado no ambiente de produção, mediante prévia autorização do responsável técnico de TIC do respectivo Órgão Setorial.
- Analisar a questão da propriedade intelectual do código-fonte quando da aquisição de uma aplicação, especialmente para as licenças de aplicações de código aberto.
- Investir em capacitação de gestão de aplicações e disciplinas correlatas para os servidores de TIC dos respectivos Órgãos Setoriais.
- Investir em capacitação de gestão e fiscalização de contratos para os servidores de TIC dos respectivos Órgãos Setoriais.
- Qualquer tipo de licença de software que for instalado nas máquinas da Prefeitura do Município de São Paulo deve ser do tipo Corporativa. Não realizar aquisição ou instalação de softwares do tipo licenças pessoais ou para Pessoa Física.
- Garantir que nenhum software que não tenha sido adquirido pela Prefeitura do Município de São Paulo seja instalado nos equipamentos da Administração Pública, ou seja, não devem ser instalados softwares com licenças pessoais ou de terceiros nos computadores da Prefeitura.

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.

CONTRATAÇÃO, ALUGUEL, ADOÇÃO OU DESENVOLVIMENTO

A tabela a seguir resume de forma extremamente simplificada o principal benefício de cada modelo de aquisição.

Modelo de Aquisição	Benefício
Contratação	Eficiência operacional para processos mais genéricos
Aluguel	Maior velocidade de colocação em produção para processos mais genéricos
Adoção	Flexibilidade com baixo custo de aquisição
Desenvolvimento	Atendimento mais preciso às regras de negócio

Tabela 17: Principal benefício dos modelos de aquisição de aplicações.

A contratação de uma aplicação é adequada para projetos que implementam processos padronizados de negócio, ainda que seja necessária alguma adequação na solução. Uma aplicação adquirida junto a bons fornecedores no mercado permite também a introdução de boas práticas dentro do Órgão Setorial. Por outro lado, deve-se ponderar a maturidade dos processos de negócio para esta alternativa.

O aluguel de uma aplicação é uma boa opção para áreas de negócio com processos padronizados, que precisam de grande agilidade para colocar as aplicações em produção e que manipulam dados de menor sensibilidade. Por outro lado, o aluguel é desencorajado em caso de

dúvidas sobre o nível de integração e customização necessárias, ou quando houver certeza de grande destes dois processos para a aplicação ofertada. A resistência a modificar os processos de negócio e/ou os modelos de dados e fontes também podem desencorajar este modelo de contratação.

A adoção de uma nova aplicação, por meio de soluções de código livre ou aberto, permite maior liberdade e flexibilidade para customização, aliado a um custo baixo ou até mesmo nulo de aquisição. Entretanto, deve-se atentar para questões de propriedade intelectual das licenças adotadas e também para a questão de manutenção e suporte. A adoção deste modelo depende do Órgão Setorial ter, em seus quadros, pessoas capacitadas nas tecnologias envolvidas na aplicação, para que a sua implementação tenha maior efetividade.

O desenvolvimento de uma nova aplicação tende a ser mais caro e com mais riscos, por conta da possibilidade de fracasso em projetos de desenvolvimento, problemas de documentação, atrasos na subida para produção ou quantidade de bugs. Assim, este modelo de aquisição é mais voltado a projetos que possuam escopo reduzido e cujos requisitos funcionais ou não funcionais sejam relativos diretamente aos processos fundamentais de negócio do Órgão Setorial, pois é baixa a probabilidade de haver soluções de mercado que atendam tais requisitos de maneira integral.

Como padrão, os Órgãos Setoriais deverão buscar uma solução pronta (mediante contratação, aluguel ou adoção) antes de optar pelo desenvolvimento. No entanto, cada Órgão Setorial deverá ponderar a decisão também pautado pela sua capacidade de gestão dos serviços ou da implantação.

A busca pela solução se dará pelas seguintes etapas:

- Avaliação de aplicações similares desenvolvidas por outros Órgãos Setoriais, mediante consulta ao Órgão Central e a um ou mais catálogos de sistemas, quando disponíveis no Portal de Governança.
- Avaliação da existência e viabilidade de adoção de software disponibilizada no Portal do Software Público Brasileiro (https://softwarepublico.gov.br/) e, eventualmente, softwares utilizados por outros entes.

- Se o Órgão Setorial conhecer uma solução de software livre ou aberto que atenda às necessidades, então esta deverá ser avaliada antes de se decidir pelo desenvolvimento.
- Avaliação da contratação de uma aplicação junto a fornecedores externos.
- Desenvolvimento interno de solução.

O Integrador Estratégico não poderá propor novos desenvolvimentos, caso tenha conhecimento da existência de aplicações similares na Administração Municipal, sem que haja prévia avaliação dos órgãos envolvidos.

O desenvolvimento e gestão de aplicações e portfólios deverá ser realizado mediante processos e critérios definidos pelo Órgão Central e, subsidiariamente, por processos e critérios definidos pelo respectivo Órgão Setorial.

O Órgão Central poderá coordenar o desenvolvimento colaborativo para atendimento das necessidades dos Órgãos Setoriais.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Para contratação de desenvolvimento por produto, definir com clareza o escopo de cada produto a ser desenvolvido.
- Para contratação de desenvolvimento com escopo aberto (ex: contratação de X pontos de função), cada aplicação deverá ter um escopo limitado e definido.
- Para contratações de desenvolvimento, prever que os direitos de propriedade intelectual e direitos autorais sobre os diversos artefatos e produtos produzidos ao longo do contrato, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados pertençam à Administração, justificando os casos em que isso não ocorrer.
- Para desenvolvimento, adotar preferencialmente iterações curtas e entregas frequentes, observando-se a metodologia adotada e a complexidade da aplicação.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Avaliar previamente à aquisição de uma aplicação, se o Órgão Setorial dispõe de servidores em quantidade e capacidade suficientes para realizar a aquisição, conforme a modalidade escolhida, bem como a eventual fiscalização e gestão dos contratos, caso aplicável.
- Adotar boas práticas e metodologias de análise e gerenciamento de requisitos.
- Adotar critérios de teste e qualidade para soluções desenvolvidas, bem como o uso de ferramentas que automatizem a validação desses critérios.
- Incluir todas as atividades inerentes ao ciclo de vida de desenvolvimento na métrica de pagamento em função dos resultados e produtos entregues.
- Evitar pagar por atividades já incluídas no escopo dos serviços aferidos pela métrica de desenvolvimento de software, como levantamento de requisitos, reuniões ou outros custos operacionais da contratada que já fazem parte dos encargos do contrato passíveis da contraprestação financeira aferida pela métrica de resultados.

RACIONALIZAÇÃO E CONSOLIDAÇÃO

Define-se como racionalização de aplicações a adequação do parque de aplicações às necessidades de negócio, de forma estruturada e planejada.

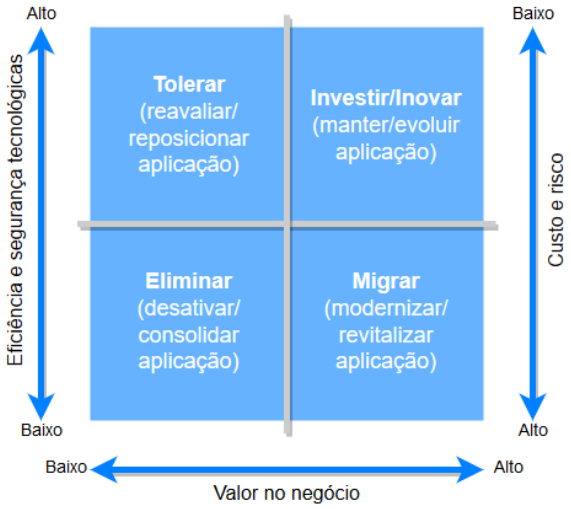
Define-se como consolidação de aplicações a fusão ou substituição de uma ou mais aplicações que possuem finalidades similares, por uma única aplicação.

O objetivo da racionalização e consolidação é maximizar a quantidade de aplicações que entregam maior valor ao negócio, ao mesmo tempo em que possuem menor custo de manutenção e operação.

Para fins de racionalização e consolidação, aplicação é a automatização de um ou mais processos de negócio, em sua totalidade ou parcialmente. Incluem-se sites que executam códigos que automatizam processos de negócio e áreas de armazenamento de dados que são manipulados por processos de negócio.

- Excluem-se aplicações de produtividade pessoal, como e-mail, calendário e processamento de texto, assim como são excluídas ferramentas clientes, tais como software antivírus e clientes VPN, bem como software de apoio à infraestrutura, como gestores de licenças, sistemas operacionais, servidores web etc.

Quatro tipos de ações podem ser adotadas para racionalização, conforme o valor no negócio, a eficiência e segurança tecnológicas e custo e risco, quais sejam: Tolerar, Investir/Inovar, Migrar e Eliminar, conforme figura a seguir.



A ação de Tolerar é dirigida a aplicações legadas que ainda entregam algum valor ao negócio, com custos e riscos aceitáveis dentro do orçamento, dos processos de negócio e das tecnologias vigentes.

- A aceitação dos custos e riscos é feita mediante avaliação técnica do responsável técnico da área de TIC do Órgão Setorial.
- Uma vez que a aplicação for enquadrada na categoria de Tolerar, ela só poderá sair dessa categoria para as ações de Eliminar ou Migrar.

A ação de Investir/inovar é voltada a aplicações mais recentes, que precisam ser atualizadas às mudanças nos processos de negócios e a aplicações cujo volume de dados dificulta a sua adequação a novas tecnologias.

- Aplicações que forem enquadradas nessa categoria serão consideradas como potenciais alvos de investimento para agregar maior valor e também para expandir e melhorar o seu uso no Órgão Setorial e/ou na Prefeitura do Município de São Paulo.

A ação de Migrar se destina a aplicações que entregam valor significativo ao negócio, mas que apresentam grandes riscos em termos técnicos, de pessoal ou de informação.

- Riscos em termos técnicos podem ser causados pelo aumento do custo em se manter o valor entregue pela aplicação ou a qualidade do serviço, por conta de fatores como documentação deficiente/inexistente, tecnologias obsoletas/incompatíveis ou complexidade crescente por conta do acúmulo de atualizações e manutenções.
- Riscos em termos de pessoal podem ser causados em função de fatores como mão-de-obra capacitada em vias de exoneração, aposentadoria ou encerramento de contrato, ou a dependência de uma única pessoa ou de um grupo reduzido de pessoas (três pessoas ou menos) para manter a aplicação.
- Riscos em termos de informação podem ser causados por informações redundantes, imprecisos ou com custo significativo para a manutenção ou a integração das informações.

- Aplicações desenvolvidas de forma ad hoc (informalmente conhecidas como sistemas caseiros ou similares) se enquadram nesta categoria por padrão.
- Aplicações que forem enquadradas nessa categoria serão consideradas como potenciais candidatas para iniciativas de consolidação, substituição ou migração de aplicações.

A ação de Eliminar é empregada a aplicações que apresentem baixo valor ao negócio ou tecnologias obsoletas/inadequadas/deficientes ou ainda a aplicações duplicadas.

- A avaliação das tecnologias é feita pelo responsável técnico da área de TIC do Órgão Setorial.
- Uma vez enquadrada na categoria de Eliminar, ela deverá ser alvo de iniciativas de desativação definitiva ou de consolidação.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Avaliar periodicamente as aplicações existentes em termos de esforços de racionalização e consolidação, mapeando as ações no seu Plano Diretor Setorial de TIC (PDSTIC) caso aplicável.
- Avaliar periodicamente o alinhamento das aplicações aos processos de negócio, identificando inclusive possíveis oportunidades de melhoria do próprio processo.
- Para aplicações da categoria Tolerar, o Órgão Setorial poderá identificar, desmembrar e atualizar partes das funcionalidades da aplicação, para que outras aplicações e processos sejam pouco afetadas, e então eliminar a aplicação.
- Para aplicações da categoria Migrar, avaliar as dependências existentes entre aplicações antes de traçar estratégicas de mitigação de risco.
- Para aplicações da categoria Eliminar, considerar a necessidade ou não de arquivamento e retenção de dados.

QUAIS SÃO AS NOSSAS SUGESTÕES?

- Considerar diferentes formas de entrega de aplicações, tais como: uso de plataformas e infraestruturas que permitam o processamento de informações de diferentes meios e formatos, tais como data marts; refatoramento das aplicações existentes em serviços ou componentes compartilhados; adição ou atualização das integrações entre aplicações.
- Para aplicações das categorias Migrar e Eliminar, identificar os custos atuais das aplicações e a sua possível projeção para os exercícios seguintes, para estimar a economia gerada pela iniciativa de racionalização.
- Adotar uma estratégia de renovação periódica de aplicações, por exemplo, substituindo todas as aplicações há 10 anos ou mais em produção por aplicações novas, para reduzir os custos e complexidades e melhorar a geração de valor para os processos de negócio.

PADRONIZAÇÃO DE APLICAÇÕES

Define-se como padronização de aplicações a escolha de uma aplicação, dentre as existentes, como padrão a ser adotada em detrimento das demais.

O objetivo da padronização é reduzir a variação de processos e aplicações comuns.

- A eliminação da variação não é necessariamente o objetivo.
- Para processos e aplicações diferenciadas, a padronização pode não ser aplicável.

O Órgão Central, em conjunto com a área central de negócio relacionada, conforme o caso, poderá definir aplicações padrão para toda a PMSP e, de maneira subsidiária, o Órgão Central poderá definir aplicações padrão para seus processos e atividades internos.

- A definição de aplicações padrão para toda a PMSP pelo Órgão Central deverá ser divulgada previamente no Portal de Governança e, caso aplicável, deverá explicitar eventuais prazos para adequação, sem prejuízo das outras formas de divulgação.

A padronização de aplicações pode ser considerada para alcançar benefícios como:

- Alcançar ganhos de escala, evitando abordagens de silo.
- Aprimorar a experiência do usuário e/ou do munícipe, simplificando formas de acesso e manipulação das informações e fortalecendo e consolidando a imagem do Órgão Setorial e/ou da Prefeitura do Município de São Paulo.
- Reduzir a duplicidade de esforços, processos e operações.
- Melhorar a consistência dos serviços fornecidos/oferecidos.
- Facilitar o remanejamento de mão-de-obra capacitada para melhorar o desempenho e reduzir os custos de atendimento das necessidades do Órgão Setorial.

A padronização de aplicação não é indicada para cenários como:

- Baixa relação benefício-custo.
- Grande diversidade de realidades e culturas atendidas pelas aplicações candidatas à padronização.
- Necessidade de diferenciação das aplicações para atender a regras ou estratégias de negócio.
- Possibilidade de desativação das regras de negócio suportadas pelas aplicações candidatas à padronização.

A avaliação para fins de padronização será feita pelo responsável técnico pela área de TIC do respectivo Órgão Setorial ou pelo Órgão Central, no caso de ser uma iniciativa de padronização que transcende o escopo de um Órgão Setorial.

QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Avaliar tecnicamente os cenários e a relação custo-benefício da padronização de aplicações, mapeando as ações no seu Plano Diretor Setorial de TIC (PDSTIC) caso aplicável.
- Avaliar periodicamente as aplicações em produção para identificar possibilidades ou necessidades de padronização.

REFERÊNCIAS

Duggan, Jim. Application Portfolio Triage: TIME for APM. Gartner, 2014. Publicado em 06 de novembro de 2014.

Duggan, Jim, Swanton, Bill, Carilton, Daryl. Analyzing the Application Portfolio for Redundancy. Gartner. Publicado em 13 de abril de 2015.

Robison, Lyn. Application Rationalization: Burning Fat and Building Muscle. Gartner. Publicado em 07 de agosto de 2006.

Swanton, Bill, Kyte, Andy, Norton, David. Apply These Best Practices for Application Consolidation. Gartner. Publicado em 02 de dezembro de 2016.

Watson, Richard. Making a Software Form-Factor Decision: Build, Borrow, Buy, or Rent?. Gartner. Publicado em 13 de junho de 2011.

Watson, Richard, Thomas, Anne. Decision Point for the Build vs. Buy Software Sourcing Decision. Gartner. Publicado em 03 de julho de 2012.

Boas práticas, vedações e orientações para contratação de software e de serviços de desenvolvimento e manutenção de sistemas (Fábrica de Software). Ministério do Planejamento, Desenvolvimento e Gestão, 2017.

Em caso de dúvidas, o Portal de Governança de TI (http://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): 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