PREFEITURA DE
SÃO PAULO

MANUAL DE ORIENTAÇÃO SOBRE PLANO DE CONTINUIDADE NO SETOR TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO EM SEGES

1ª EDIÇÃO - 2026

PREFEITURA DE
SÃO PAULO

PREFEITURA DE SÃO PAULO

Prefeito
Ricardo Nunes

SECRETARIA MUNICIPAL DE GESTÃO

Secretária
Marcela Arruda

Secretária Adjunta
Regina Silverio

Chefe de Gabinete
Thaís Rodrìgues

COORDENADOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
Wagner Santana Silveira

REDAÇÃO
Davi Giugno
João Victor Silva
Rafael da Matta

DIAGRAMAÇÃO
Bianca Abreu
Carolina Teixeira

REVISÃO
Roseli Andrade Pires

SUMÁRIO

GLOSSÁRIO

Acesso: Refere-se a um nível de funcionalidade de um serviço ou dados a que o usuário possui direitos de acesso e uso.

ANPD: A Autoridade Nacional de Proteção de Dados (ANPD) é uma autarquia federal de natureza especial do Brasil que, atualmente, se encontra vinculada ao Ministério da Justiça e Segurança Pública e possui atribuições relacionadas a proteção de dados pessoais e de privacidade.

ASCOM: Assessoria de Comunicação - ASCOM é o órgão responsável pelo planejamento, coordenação e execução da política de comunicação social da Secretaria Municipal de Gestão, em consonância com a Secretaria Especial de Comunicação da Prefeitura de São Paulo.

Backup: Termo utilizado para uma atividade que consiste em realizar cópias de segurança de dados digitais de um dispositivo.

COTIC: Coordenadoria de Tecnologia da Informação e Comunicação

LGPD: A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade, e a livre formação da personalidade de cada indivíduo.

Logins: Perfis de acessos.

Malware: Malware é qualquer software intencionalmente feito para causar danos a um computador, servidor, cliente, ou a uma rede de computadores.

Phishing: Phishing é uma técnica de engenharia social usada para enganar usuários de internet usando fraude eletrônica para obter informações confidenciais.

PMSP: Prefeitura Municipal de São Paulo.

Prodam: Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo, de economia mista, é a parceira tecnológica da Prefeitura de São Paulo e integradora estratégica de soluções inovadoras de tecnologia da informação e da comunicação.

PSI: Refere-se a portaria da Política de Segurança da Informação, da Secretaria Municipal de Gestão.

RH: Recursos Humanos.

SEGES: Refere-se a Secretaria Municipal de Gestão.

SEI: O Sistema Eletrônico de Informações (SEI) é um sistema desenvolvido pelo Tribunal Regional Federal da 4ª Região. Usada também em outras instituições públicas, como sistema de gestão de processos e documentos eletrônicos.

SIGPEC: Sistema Integrado de Gestão de Pessoas e Competências, é um sistema informatizado cuja arquitetura integra os eventos da área de Recursos Humanos, tratados durante mais de 30 anos (contados até junho de 2008) por diversos sistemas independentes.

SLAs: Acordo de Nível de Serviço.

SUPRI: O sistema SUPRI possui um banco de preços para materiais de consumo, relacionando todos os preços mínimos e máximos registrados nos estoques dos Almoxarifados, estabelecendo a moda e a frequência dos preços mais praticados.

TIC ou TI: Refere-se a tecnologia da informação e comunicação.

Vírus: Um vírus de computador é um tipo de programa malicioso que se propaga através de computadores e dispositivos conectados em rede, por meio de downloads de arquivos infectados, anexos de e-mail maliciosos, sites comprometidos, dispositivos de armazenamento e outros tipos de arquivos infectados.

INTRODUÇÃO

Nosso objetivo foi o de criar um Plano de Continuidade de Negócios (PCN) para a SEGES – Secretaria Municipal de Gestão - da PMSP. A SEGES é uma secretaria-meio. A pasta fornece condições e diretrizes para as demais secretarias funcionarem. Processos administrativos importantes estão sob a égide da secretaria, tais como gestão de carreira, de licenças médicas de servidores e de folha de pagamento, além da elaboração de normativos tanto internos à própria SEGES quanto relativos às demais secretarias. Assim, muitos desses processos dependem de ativos de TIC para poderem ser executados, seja na forma de rede corporativa, de sistemas de informação variados, de espaços de armazenamento e mesmo de hardware.

Para que as funções vitais da SEGES não sofram solução de continuidade quando da ocorrência de desastres com ativos de TIC, é necessário que haja planos de contingência e de continuidade de negócios vigente na Secretaria, que determine claramente o que deverá ser feito para o restabelecimento da normalidade das operações.

Um plano de continuidade de negócios (PCN) foca na restauração rápida das funções críticas de uma organização após um evento disruptivo. Ele deve identificar as operações essenciais para o funcionamento da organização e definir a forma como essas operações serão recuperadas em caso de interrupção.

Este PCN vem complementar a Política de Segurança da Informação - PSI da SEGES, conforme estabelecido no Art.2 da referida política, e tem ligação com o Manual de Orientação sobre Gestão de Risco no Setor Tecnologia da Informação e Comunicação em SEGES e ao Manual de Orientação de Acessos de Tecnologia da Informação e Comunicação em SEGES, também derivado da PSI.

1. ANÁLISE DE IMPACTO NOS NEGÓCIOS

1.1 Identificar os serviços e funções críticas dos recursos de TIC da Secretaria

Os sistemas de informação mais críticos são o SEI, o SIGPEC e o SUPRI. São sistemas que são usados continuamente em uma ampla gama de funções e são atualizados em tempo real, de modo que sua paralisação pode ter consequências graves para as atividades da Secretaria.

Outro recurso de TIC essencial para as operações cotidianas da SEGES é a rede corporativa, utilizada por todos os seus servidores e que permite acesso não só a sistemas de informação, mas também a ferramentas como e-mail corporativo, aplicativos corporativos de troca de mensagens (como o Teams) e espaços de armazenamento de arquivos e de pastas de arquivos.

Por fim, temos as diversas bases de dados de que a SEGES é proprietária, especialmente aquelas que estão vinculadas aos sistemas de missão crítica citados anteriormente nesta seção.

1.2 Avaliar os impactos potenciais de interrupções, incluindo custos e efeitos no bem-estar dos servidores

Explicaremos aqui os impactos para a SEGES e seus servidores, em caso de falhas nos recursos de TIC apontados na seção anterior.

O SEI gerencia documentos e processos administrativos na PMSP, muitos com prazos e níveis de urgência. Sua interrupção pode atrasar decisões e atividades importantes.

O SIGPEC é um sistema de gestão de RH, que cobre muitas áreas da vida funcional dos servidores, como gestão de frequência, de férias, de licenças, de progressão de carreira, contagem de tempo, dentre outros processos. Chega a ser importante ao ponto de enviar dados de servidores para folhas de pagamento. Com tamanha carga de funções essenciais, não é difícil percebermos que a queda do SIGPEC causaria grande transtorno nas atividades corriqueiras da Secretaria.

O SUPRI cuida da gestão de suprimentos em tempo real, e sua queda ou paralisação também poderá acarretar problemas diversos para a Secretaria, especialmente em questões de estoques e almoxarifado.

Pelos apontamentos acima, resta justificado o porquê de os três sistemas de informação aqui citados – SEI, SIGPEC e SUPRI - serem aqueles com missão mais crítica em SEGES.

No que toca a quedas na rede corporativa, tudo dependerá da duração da queda e de quais áreas exatamente foram afetadas. Uma coisa é haver uma queda por alguns minutos em um setor específico, causando apenas um ligeiro atraso em algumas tarefas e um incômodo passageiro para alguns servidores. Outra coisa é uma queda por várias horas e que atinja a totalidade ou quase totalidade da SEGES. Neste último caso, há uma paralisação quase total das atividades habituais da Secretaria, desde as mais simples – como envios de mensagens e respostas a e-mails - até processos críticos como cômputo de frequências, registro de perícias médicas, assinaturas de decretos e portarias, com todas as consequências negativas daí advindas.

Raciocínio semelhante pode ser elaborado para situações de queda de energia que se estendam por longo tempo, geralmente por mais de um par de horas.

Mas poucos cenários seriam piores do que o vazamento – intencional ou não - de dados sigilosos ou sensíveis da Secretaria, mediante acesso - autorizado ou não - às bases de dados de sua propriedade. As consequências legais e institucionais poderão ser bastante desastrosas, especialmente se as diretrizes contidas na LGPD para lidar com tal situação não forem seguidas. Danos severos à imagem da SEGES, advindos de tal vazamento, seriam igualmente difíceis de reparar, pois tais reparos demandariam bastante tempo e esforço. Para não falar de eventuais prejuízos financeiros que poderiam ocorrer, seja diretamente na forma de sanções pecuniárias e indenizações aos atingidos pelos vazamentos, seja indiretamente, na forma de uma maior dificuldade de se realizar certames licitatórios, parcerias e contratações, motivada pela confiança reduzida de agentes externos, como empresas e organizações do terceiro setor, na Secretaria, ao menos por algum tempo após o incidente.

Cenário igualmente desastroso seria o da perda de tais bases de dados, por qualquer motivo que seja, desde dano grave nos dispositivos de armazenamento das bases até acesso autorizado (ou não) com destruição intencional dos dados. Uma forma de mitigar este risco específico seria garantir a existência de um backup – plenamente operacional – de cada base de dados crítica para os negócios da SEGES, em local distinto da base de dados original.

1.3 Definir o tempo máximo admissível de interrupção para cada serviço

Temos contratos com a PRODAM que regem os serviços de Datacenter e Infraestrutura, além de contratos para o desenvolvimento de soluções de TIC específicas, como sistemas de informação, integrações entre softwares, e serviços similares. Estes contratos, via de regra, têm acordos de níveis de serviço, que determinam quando e como o suporte da empresa pode ser acionado em caso de necessidade, bem como definem penalidades em caso de não-cumprimento, pela empresa, dos níveis de serviço acordados.

Pode haver contratos semelhantes com outras empresas que nos forneçam serviços e produtos específicos de TIC, além da PRODAM. Para estas empresas, vale o mesmo raciocínio aplicado à PRODAM, que é o de estabelecimento de acordos de níveis de serviço a serem cumpridos por elas.

Vale recordar que, conforme os nossos contratos com os prestadores de serviços são aditados ou renovados, os níveis mínimos de serviço podem sofrer alterações. Esta é uma das razões pelas quais este documento e outros documentos ligados à PSI da SEGES, bem como a própria PSI, podem ser periodicamente revisados.

2. AVALIAÇÃO DE RISCOS

2.1 Identificar potenciais ameaças

Entre as principais ameaças identificadas em SEGES com potencial para causar paralisações severas nas atividades da Secretaria, listamos:

- Acesso não autorizado à rede corporativa;
- Falta de conexão com a internet corporativa por períodos longos;
- Falta de energia por períodos longos;
- Paralisação de um sistema de informação, especialmente de um sistema estruturante, como aqueles citados neste texto;
- Perda de bases de dados, sejam eles confidenciais, sensíveis ou não;
- Vazamento de dados sensíveis ou confidenciais de propriedade da Secretaria;
- Vírus, phishing e malware que invadam sistemas de informação estruturantes ou bases de dados sensíveis ou confidenciais, podendo incorrer nas duas ameaças anteriores.

2.2 Avaliar a probabilidade e o impacto de cada ameaça

De acordo com o Plano de Gestão de Riscos, que também integra nossa Política de Segurança, temos uma matriz de risco – Risco Inerente, na verdade - que contempla as dimensões de probabilidade – de muito baixa a muito alta – e impacto, de muito baixo a muito alto. Aqui reproduzimos apenas aqueles itens com risco inerente considerado alto ou extremo, mais um risco Moderado específico – o de queda de energia elétrica - justamente por terem potencial de paralisar ou atrapalhar de forma severa as atividades da Secretaria.

Evento	Risco Inerente Associado	Tratamento do Risco	Existe a medida de tratamento em SEGES?
Perda de bases de dados	Extremo	Existência de backups operacionais das bases; Armazenamento seguro das bases e de seus backups; Controle severo de acesso às bases de dados; Medidas contra malware, vírus e phishing.	Existe política de backup seguindo Orientação Técnica do Orgão Central
Vazamento de dados sensíveis e/ou sigilosos	Extremo	Controle severo de acesso a bases de dados e sistemas de informação; Medidas contra malware, vírus e phishing; Não deixar informações sensíveis à mostra, etc.	Aplicar passos determinados na Política de Segurança da Informação
Queda da Internet	Alto	Redundância de links de acesso e de provedores	Acionamento da Prestadora de Serviços.

Queda de Força	Moderado	Hábito de fazer backups frequentes de documentos e trabalhos importantes; Uso de no-breaks e geradores.	Não possui atualmente
Vírus, malware, phishing	Muito Alto	Antivírus atualizado; Campanhas educativas para colaboradores.	Isolamento do equipamento da rede Corporativa e formatação do equipamento.
Paralisação de sistemas estruturantes	Alto	Pronta abertura e acompanhamento de chamados com a Prestadora; Acesso a backups de bases de dados dos sistemas afetados; Redundância de servers e bases de dados na PRODAM.	Em SEGES só podemos abrir e acompanhar chamados com a Prestadora;. Demais medidas competem à Prodam.
Vandalismo e furto/roubo	Alto	Controles de acesso físico; Guardar equipamentos como notebooks, tablets e afins em local seguro. Fazer BO.	Contratação de segurança predial; Em caso de furto/roubo acionar CAF.

3. ESTRATÉGIA DE RECUPERAÇÃO

3.1 Estabelecer medidas preventivas e de mitigação.

A maior parte das medidas preventivas está coberta pelo material do Manual de Gestão de Riscos, que também está vinculado à Política de Segurança de SEGES.

3.2 Determinar recursos necessários para a recuperação

Para os sistemas de informação críticos, como os já citados SEI, SIGPEC e SUPRI, a primeira medida a ser tomada, caso algum deles saia do ar ou apresente falha grave que impossibilite o seu uso normal, a medida inicial será abrir chamado junto à PRODAM, que hospeda os recursos de Datacenter que sustentam tais sistemas.

Se o problema ainda assim persistir, ou se a solução demorar mais do que o estipulado por SLAs para entrar em operação, aplicar penalidades à Prodam, seguindo os ritos já estabelecidos para tanto.

Para casos de queda da rede corporativa por prazo superior a 1 hora, seguir roteiro similar.

Os atuais SLAs com a Prodam preveem disponibilidade de 99,741% do tempo - Tier II – para o Datacenter, com direito a 48 horas anuais de parada para manutenção programada. Tais paradas deverão ser comunicadas pela Prodam à SEGES com antecedência de 20 dias.

Para serviços de Redes e Conectividade, os termos são de disponibilidade de 99,7% do tempo, também com direito a 48 horas anuais de parada para manutenção programada. Tais paradas deverão ser comunicadas pela Prodam à SEGES com antecedência de 20 dias.

4. DESENVOLVIMENTO DO PLANO

4.1 Detalhar as ações, responsabilidades e prazos para cada função crítica.

4.1.1 Detalhamento das Responsabilidades

Gabinete da SEGES: Aprovar os planos de continuidade propostos pela COTIC e principal interessada das atividades críticas da SEGES.

COTIC: Elaborar e revisar a documentação de Continuidade de Negócios de TIC produzida pela COTIC, e executar as medidas contidas no referido Plano, sempre informando o Gabinete sobre os procedimentos adotados e sobre o status do Plano.

ASCOM: Poderá, quando solicitada, comunicar aos usuários a ocorrência de eventos que comprometem seriamente as atividades principais da Secretaria, bem como informará as medidas que vêm sendo tomadas – resguardadas aquelas que eventualmente requeiram sigilo – para remediar a situação. Poderá também informar aos usuários o retorno à situação de normalidade, a depender da situação.

4.2 Estabelecer Cursos de Ação e Protocolos de comunicação interna e externa.

Não é possível separar completamente as medidas de contenção de desastres dos protocolos de comunicação, na maioria das vezes. Isto porque entre etapas sucessivas de ação e contenção, pode ser necessário algum tipo de comunicação de COTIC com as demais áreas e atores afetados e envolvidos no problema.

Isto posto, passemos ao protocolo geral de ação e comunicação a ser seguido em COTIC no caso de situações com potencial para causar severa ruptura nas atividades normais da SEGES, ou que, mesmo não causando tal ruptura, sejam suficientemente graves para pedir ação imediata.

4.2.1 Protocolo Geral de Ação e de Comunicação de Incidentes de TIC

O protocolo geral de ação e comunicação aqui exposto no caso de quedas de internet, bem como de falhas graves ou mesmo quedas em sistemas de informação estruturantes. Com algumas adaptações, pode ser utilizado para situações de queda de energia elétrica, mas NÃO se aplica a cenários de perda ou vazamentos de dados de posse da SEGES, ou a problemas como acesso indevido à rede, ou a questões de vandalismo/furto/roubo de equipamentos. Nestes casos, que serão cobertos mais adiante, o protocolo é específico para cada situação.

- Acionamos o fornecedor do serviço para tratativas – geralmente a abertura de chamados é o primeiro passo - e é evocado o SLA contratual, de acordo com a criticidade do problema;
- Comunicamos primeiramente os coordenadores de SEGES, via WhatsApp/Microsoft Teams, para avisar as equipes sobre o ocorrido;
- Após decorridas 2h do início do incidente, sem ter havido a solução, passamos um novo posicionamento às áreas internas de SEGES;
- Após decorridas 4h do início do incidente, sem ter havido a solução, enviamos um novo comunicado às áreas internas de SEGES e estipulamos um novo horário para envio de novos comunicados;
- Tal protocolo de comunicação repete-se até a solução do problema;
- Após a solução do problema, enviamos um comunicado onde se explica a causa do problema e, em paralelo, reunimos evidências para penalizar a fornecedora do produto ou serviço, sempre observando o SLA e demais termos contratuais que temos com tal fornecedora.

Para o caso específico de falta de energia, modifica-se o procedimento acima, resultando na seguinte linha de ação:

- Este item fica fora do escopo de ação de COTIC. O que pode ser feito é acionar a CAF/DIAP, que atualmente é a divisão da SEGES que fiscaliza serviços de energia elétrica, a fim de que tal divisão encaminhe as devidas providências.

4.2.2. Outros Cursos de Ação e Protocolos de Comunicação

No caso de vandalismo/furto/roubo de equipamentos:

- Apuração inicial dos fatos, com todos os dados que for possível coletar acerca do(s) equipamento(s) atingido(s), do local e data/hora do ocorrido e o que mais couber;
- Com os dados acima, lavrar Boletim de Ocorrência (BO) em órgão policial competente;
- Abrir processo administrativo, para averiguação de responsabilidades.

Lembrando que tal situação, em geral, não costuma causar ruptura em atividades-chave de SEGES. Porém, consta deste Documento pela gravidade de que uma tal situação se reveste, exigindo medidas imediatas. A gravidade poderá escalar no caso de vandalismo/furto/roubo de equipamento contendo, em seus dispositivos de armazenamento, dados pessoais sensíveis ou confidenciais da SEGES.

4.2.3 - Protocolo a ser seguido para casos de Incidentes de Segurança da Informação envolvendo Dados Pessoais Sensíveis ou Dados Confidenciais

A identificação e classificação de incidente de segurança que envolva dados pessoais deverá ser realizada pela área responsável, com posterior encaminhamento ao Gabinete (GAB), que decidirá sobre o envio à Controladoria Geral do Município (CGM), órgão responsável pelo papel de controlador no âmbito da PMSP.

O monitoramento e o tratamento de incidentes deverão respeitar integralmente as normas vigentes, especialmente a Lei Geral de Proteção de Dados (LGPD) e as normas emitidas pela Controladoria Geral do Município (CGM), garantindo a inviolabilidade de informações e dados pessoais sensíveis ou que envolvam aspectos de intimidade e privacidade de pessoas.

Para fins de eventual fiscalização e controle do monitoramento pela CGM, a COTIC deverá manter registro integral das atividades de monitoramento e resposta ao incidente.

4.3 Definir locais de recuperação alternativos

Atualmente a SEGES não dispõe de DATACENTER próprio, sendo que os serviços de Datacenter são contratados junto a empresas especializadas, visando mitigar riscos de segurança, disponibilidade e outros. Em tais contratos, ficam previstos, por meio de cláusulas específicas, os níveis de serviço (SLAs) requeridos e quaisquer questões relativas à continuidade dos serviços prestados.

5. TREINAMENTO E TESTES

5.1 Treinar os servidores sobre seus papéis no plano.

Com relação aos treinamentos, podemos considerar dois grupos de colaboradores em SEGES: o pessoal de COTIC e o pessoal das demais áreas da Secretaria.

Para o pessoal de COTIC, recomenda-se o treinamento mais intensivo e aprofundado, no intuito de cobrir todas as situações ligadas a ativos de TIC que ponham em risco atividades-chave da Secretaria, como queda de internet, de força, de sistemas estruturantes e mesmo de vazamento ou perda de dados confidenciais ou sensíveis. Todos os procedimentos em cada uma dessas situações devem ser cobertos e conhecidos por todos os servidores de COTIC. Tais procedimentos são recomendados, podendo ser periodicamente recapitulados e mesmo revisados, contando com a participação e conhecimento de todos.

Para os colaboradores de SEGES, o essencial é saber que existe um plano de continuidade de negócios de TI e, em situações cobertas pelo plano, agir conforme recomendado por COTIC e Gabinete da Secretaria. Reportar possíveis incidentes ligados a dados sensíveis e/ou sigilosos da Secretaria, bem como reportar à COTIC problemas nos sistemas de informação estruturantes em uso, na rede corporativa e mesmo suspeitas de acesso não-autorizado à rede corporativa, pelos canais disponíveis na ocasião.

Campanhas educativas junto aos servidores de SEGES, promovendo a conscientização dos mesmos em assuntos de segurança da informação, poderão ter a colaboração da COTIC, da ASCOM e do Gabinete da Secretaria.

5.2 Realizar simulações e exercícios regulares para testar a eficácia do plano e identificar pontos de melhoria.

Estes exercícios podem ser realizados internamente em COTIC, em ocasiões e locais que não atrapalhem o fluxo normal de atividades da Secretaria.

6. MANUTENÇÃO E REVISÃO

6.1 Atualizar o plano regularmente, considerando mudanças na infraestrutura, pessoal e contexto da Secretaria.

Este PCN poderá ser revisado periodicamente, ou sempre que a situação da Secretaria assim o ensejar, ou mesmo após algum incidente de segurança de informação, caso necessário.

Uma sugestão é realizar as revisões deste PCN a cada 24 ou 36 meses, no máximo.

6.2 Rever o plano após cada teste ou incidente real para incorporar aprendizados.

Este ponto é de grande importância, pois este PCN não é uma obra acabada, mas sim um documento em constante evolução. Recomenda-se sempre atualizá-lo à medida que temos aprendizados novos, seja após incidentes de segurança da informação, testes e treinamentos, mudanças eventuais em normativos da PMSP, da própria Secretaria ou de outras esferas - como a legislação estadual e mesmo a federal – e também por ocasião de avanços tecnológicos que ensejem novos desafios para a segurança da informação em SEGES.

7. COMUNICAÇÃO

A comunicação é extremamente importante em um PCN, pois garante que todos os lados afetados por um evento de segurança de informação estejam a par dos fatos ocorridos e sejam orientados a tomar as medidas corretas para mitigar seus efeitos até a restauração da normalidade.

Os protocolos de comunicação já foram estabelecidos na seção 4 deste Documento para diversas situações que podem eventualmente atingir a SEGES, de modo que aqui são feitas considerações de ordem mais geral.

7.1 Garantir que todos os servidores, parceiros e fornecedores estejam cientes do plano e saibam como se comportar em uma situação de crise.

As áreas competentes em SEGES, tais como COTIC, Gabinete e mesmo a ASCOM, compete comunicar eventos ligados à segurança da informação, especialmente nas situações descritas neste PCN, aos servidores, bem como comunicar os servidores o retorno à normalidade após as situações críticas que tenham ocasionado o acionamento do PCN.

7.2 Utilizar canais de comunicação diversos, incluindo mídias sociais, sites e meios tradicionais, para atualizações em tempo real durante crises.

A comunicação tratada no item 7.1 acima poderá ser feita pelos meios julgados mais convenientes, sejam os meios corporativos tradicionais, como e-mail e chat corporativo, até sites e mídias sociais, a depender da situação. Casos mais graves, como incidentes com dados pessoais sensíveis ou sigilosos, poderão exigir comunicação mais ampla, como aquela fornecida pelas mídias sociais e pelo site da SEGES.

PREFEITURA DE
SÃO PAULO