PREFEITURA DE SÃO PAULO

MANUAL DE ORIENTAÇÃO DE ACESSOS DE 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.

API: interface de programação de aplicações.

Ativos intangíveis: Os ativos intangíveis são bens que não podem ser tocados, ou seja, não possuem existência física.

COTIC: Coordenadoria de Tecnologia da Informação e Comunicação

Direitos: Refere-se aos privilégios que o acesso do usuário tem a determinadas funcionalidades ou dados.

Identidade: É a forma pela qual o usuário é identificado na Secretaria. É necessariamente único para cada indivíduo.

IP: refere-se a um endereço exclusivo que identifica um dispositivo na internet ou em uma rede local, ou seja, um protocolo de rede.

Logins: Perfis de acessos.

Gerenciamento de acessos: Processo que a área de TIC realiza no intuito de regulamentar e controlar os acessos dos usuários aos recursos - físicos e lógicos - de TIC da Secretaria, observando as normas e princípios dispostas na Política de Segurança da Informação - PSI – desta mesma Secretaria. Este manual de controle de acessos fica desde já submetida à referida PSI.

PMSP: Prefeitura Municipal de São Paulo.

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

Scripts: Refere-se a códigos de programação que reúne instruções para que o computador execute.

SEGES: Refere-se a Secretaria Municipal de Gestão.

Serviços/Grupo de Serviços: Conjunto de serviços semelhantes que podem ser agrupados em perfis de acesso.

Serviços de Diretório: Ferramenta usada para gerenciar os privilégios dos acessos dos usuários.

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

INTRODUÇÃO

Este documento é derivado da PSI de SEGES, conforme estabelecido no Art. 2º da referida política, e tem por fim complementá-la em pontos relativos a riscos cotidianos de TIC em SEGES.

Este documento está igualmente ligado ao Manual de Orientação sobre Gestão se Risco no Setor Tecnologia da Informação e Comunicação em SEGES e ao Manual de Orientação sobre Plano de Continuidade no Setor Tecnologia da Informação e Comunicação em SEGES, documentos igualmente derivados da Política de Segurança da Informação (PSI) de SEGES.

1. OBJETIVO

Este manual de controle de acessos tem por finalidade regulamentar os procedimentos e privilégios de acesso aos recursos físicos e lógicos de TIC da Secretaria, o que inclui a rede corporativa, os serviços de comunicação e os sistemas de informação em uso na SEGES, assim como as máquinas, equipamentos e as instalações onde os mesmos se encontram.

1.1 Atribuição do objetivo

É dever de todos os servidores de SEGES, independentemente de seu nível hierárquico, tomar ciência do presente manual de controle de acesso de TIC, observando todas as suas recomendações e diretrizes.

É igualmente imperioso que todos os servidores de SEGES promovam ativamente as orientações do manual de controle de acessos da TIC em suas atividades rotineiras, de modo a estabelecer-se, na Secretaria, uma cultura de controle de acessos, visando a segurança física e cibernética de todos.

1.2 Comunicação do objetivo

A SEGES fará comunicações com os servidores para orientá-los quanto às melhores práticas relativas ao controle de acessos, sempre que necessário.

A transmissão ou recebimento de conteúdo ou informações institucionais será realizada exclusivamente pelos serviços corporativos da SEGES.

2. RESPONSABILIDADES

2.1 Atribuições de COTIC

2.1.1 No que toca especificamente ao controle de acessos, caberá à Coordenadoria de Tecnologia da Informação e Comunicação (COTIC):

2.1.1.1 Atribuir cada conta de acesso a computadores e demais ativos físicos de TIC da Secretaria a um responsável identificável como pessoa física, sendo que:

a) os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário;

b) os usuários (logins) de estagiários/terceiros serão de responsabilidade do gestor da área contratante.

2.1.1.2 No caso de contas de acesso a sistemas de informação, aplicativos e bases de dados em uso pela Secretaria, encaminhar a solicitação para os responsáveis pelo sistema, aplicativo ou base de dados em questão.

2.1.2 Os perfis de acesso e permissões concedidas aos usuários restringir-se-ão ao mínimo necessário para a realização das atividades profissionais previstas. Ainda neste contexto de perfis de acesso e permissões, recomenda-se haver um processo de gerenciamento de perfis de acesso, inclusive com a previsão de retirada e desativação de perfis/permissões para as situações em que tal procedimento seja necessário.

2.1.3 Os dados referentes a acessos de usuários, conteúdo trafegado a partir da rede corporativa, uso de ativos intangíveis, armazenamento de informações, marcas e recursos de TIC, além de seus ambientes físicos e lógicos, poderão ser monitorados.

2.1.3.1 Os registros de logins, e-mails, acessos a sítios de internet, histórico de navegação, endereçamento IP, condições aceitas e quaisquer outras informações relevantes poderão ser armazenados em ambiente seguro para análise posterior, se necessário.

2.1.3.2 É vedada qualquer tentativa de alteração de registros de logins, permissões de acessos e recursos físicos de TIC dos quais somente poderão ser acessados por profissionais autorizados ou pelo responsável adequado na investigação ou apuração de incidente de controle de acesso, de segurança da informação, cometimento de infração, ato ilícito ou descumprimento de lei ou norma da SEGES.

2.2 Gestores das unidades e dos sistemas de informação

2.2.1 Os responsáveis pelos ativos de TIC devem rever os direitos de acesso dos usuários em intervalos de tempo regulares.

2.2.1.1 O disposto no título 2.2.1 deste manual é válido especialmente por ocasião de alterações nas atribuições rotineiras dos usuários sob sua responsabilidade, particularmente quando implicam mudança na utilização de repositórios digitais, bases de dados, sistemas de informação, redes e outros recursos que demandem algum tipo de controle de acesso.

2.2.2 Os direitos de acesso de todos os servidores, estagiários e de terceiros à rede corporativa, aos sistemas de informação e aos recursos de TIC da SEGES devem ser removidos logo após o término do vínculo com a Secretaria, quer por exoneração, desligamento, transferência, falecimento ou qualquer outro motivo.

2.2.2.1 Em casos urgentes, o coordenador da respectiva área comunicará tal fato à COTIC, a fim de que essa providência seja tomada;

2.2.2.2 Em casos não urgentes, o fato poderá ser comunicado à COTIC pelas vias habituais em uso na Secretaria;

2.2.2.3 O disposto no título 2.2.2 vale também para quaisquer logins e senhas de acesso associados aos usuários, quando do término de seus vínculos com a Secretaria.

2.2.3 O acesso à informação e às funções de sistemas aplicativos deve ser restrito de acordo com a política de controle de acesso.

2.2.3.1 Cada colaborador só deve ter acesso aos sistemas de informação e às redes e recursos de TIC que forem realmente necessários para a realização de suas tarefas, e mesmo assim somente com os níveis de acesso estritamente necessários.

2.2.3.2 Quando cabível, o acesso a sistemas de informação e aplicações deve ser controlado por um procedimento seguro de login.

2.3 Atribuições dos usuários

2.3.1 O usuário declara desde logo conhecer, aceitar e respeitar as regras e penalidades envolvidas na utilização desta rede, abaixo descritas:

a) A senha de acesso é pessoal e intransferível, sendo o usuário o único responsável por qualquer ato, legal ou ilegal, que tiver lugar durante seus acessos à rede corporativa da Secretaria;

b) Zelar pelo uso adequado dos recursos computacionais em qualquer circunstância, respeitar a privacidade, a confidencialidade e a integridade das informações da Secretaria e de outros usuários;

c) A guarda dos documentos digitais na estação de trabalho é de responsabilidade do servidor, sendo disponibilizado pela SEGES o serviço de ambiente seguro para armazenamento;

d) Manter em sua estação de trabalho somente com os softwares homologados pela área técnica;

e) Caso seja necessária autenticação ou autorização para atualização de software homologado em sua estação de trabalho, informar a COTIC;

f) Sempre que sair da estação de trabalho, manter o usuário bloqueado;

g) Todos os acessos efetuados pelo usuário e as informações por ele manipuladas (sistema de informação, e-mails, documentos, etc.), serão passíveis de verificação pelos representantes de COTIC que recebam atribuição para tal, a qualquer momento, independente de aviso prévio.

h) Em decorrência do disposto no item anterior, o usuário declara estar ciente de que tanto a COTIC quanto a SEGES são as legítimas proprietárias e custodiantes de todos os equipamentos, infraestrutura e sistemas de informação que serão utilizados;

i) Quanto ao uso de senhas de acesso, seguir o disposto no Capítulo III desta Política;

j) Não deixar relatórios, papéis, anotações, disquetes, CDs, DVDs, pen-drives, HDs externos ou quaisquer outras mídias com informações confidenciais em cima das mesas ou em local de fácil acesso;

k) Todos os recursos de TIC disponibilizados ao usuário são para fins relacionados única e exclusivamente às atividades profissionais do mesmo em SEGES. Assim sendo, é expressamente proibido o uso de tais recursos de TIC para outros fins.

2.3.2 Fica vedado a qualquer usuário utilizar ou tentar utilizar a identidade de outro usuário na rede corporativa da SEGES, independentemente do propósito.

2.3.2.1 O usuário deverá reportar qualquer suspeita de violação de Controle de Acesso ao canal de comunicação à COTIC, tão logo quanto possível.

2.3.2.2 O tratamento do incidente reportado será objeto do título 7. AVERIGUAÇÃO DE INCIDENTES.

2.3.3 É vedada qualquer tentativa de adquirir, reproduzir, instalar, utilizar e/ou distribuir cópias não autorizadas de softwares ou programas de aplicativos, sem a permissão de COTIC.

3. SENHAS E DEMAIS CONTROLES DE ACESSO LÓGICOS

3.1 A criação do perfil (login) é essencial para controlar o acesso dos usuários a diversas aplicações corporativas e evitar que pessoas alheias àquele serviço tenham acesso a informações de forma indevida. Com tal login, é possível também acessar um conjunto de recursos e ferramentas disponíveis na rede municipal, tais como impressoras, pastas compartilhadas e internet.

3.1.1 É proibido o compartilhamento de login para funções de administração de sistemas;

3.1.2 A COTIC responde pela criação da identidade lógica na rede para os usuários, nos termos do procedimento para Gerenciamento de Contas de Grupos e Usuários.

3.2 Devem ser distintamente identificados os usuários regulares, isto é, a cada usuário será associado um único login, distinto dos demais. Ao realizar o primeiro acesso ao ambiente de rede local, recomenda-se que o usuário troque imediatamente a sua senha, conforme as orientações a seguir:

a) A senha precisa ter no mínimo 8 (oito) caracteres, e precisa também ter caracteres maiúsculos, minúsculos, números e - se possível - caracteres especiais (por exemplo: \!\@\#\$\%\¨);
b) A senha não pode conter parte do nome ou sobrenome do usuário;
c) A senha nova não pode repetir alguma das últimas 24 (vinte e quatro) senhas utilizadas;
d) A senha deve ser alterada a cada 60 (sessenta) dias, e pode ser alterada novamente após 2 (dois) dias;
e) A senha deve ser alterada em todos os dispositivos móveis.

3.3 Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários, notadamente em situações como exoneração, desligamento, transferência, falecimento, etc., conforme disposto no título 2.2.2.

3.4 Caso o usuário esqueça sua senha, tal fato deverá ser comunicado à COTIC para que seja possível a obtenção e o cadastro de uma senha nova.

3.5 Caso haja sistemas de gerenciamento de senhas em uso na Secretaria, estes devem assegurar a qualidade das senhas.

3.6 O uso de programas utilitários que possam ser capazes de sobrescrever controles de acesso a sistemas e aplicações deve ser restrito e estritamente controlado.

3.7 É recomendado evitar, tanto quanto possível, o uso de mecanismos de autopreenchimento de logins e senhas, por motivos de segurança.

3.8. É fortemente recomendado o uso de MFA (múltiplos fatores de autenticação) para sistemas de informação considerados críticos, seja por sua importância para o dia a dia da SEGES, seja por possuírem dados considerados confidenciais ou sensíveis.

3.9 Recomenda-se, tanto quanto possível, que contas com grau elevado de permissões (administrador de sistema, serviço, administrador local de máquina, aplicações e break-glass ou emergência) sejam cobertas por um Gerenciamento de Acessos Privilegiados ou PAM, na sigla em inglês. Esse PAM pode assumir a forma de:

- Descoberta e gerenciamento de contas;
- Cofre de senhas;
- Acesso just-in-time;
- Monitoramento de sessões;
- Auditoria e conformidade.

3.10. Recomenda-se o uso de um Termo eletrônico de responsabilidade quando da alocação de contas com privilégios elevados, e de trilhas de auditoria para concessões/alterações de graus de acesso/privilégios;

3.11. Recomendável haver também um ciclo JML (joiner/mover/leaver) de gestão de acesso dos servidores e colaboradores da SEGES, passando pela admissão em SEGES, mudança de função/setor e desligamento, automatizando todos os procedimentos de

4. SOLUÇÕES DE TIC DESENVOLVIDAS INTERNAMENTE

4.1 Os programas e aplicativos desenvolvidos localmente em SEGES levarão em conta, desde sua concepção, procedimentos e boas práticas em vigor sobre controles de acesso de usuários.

4.2 O acesso ao código-fonte dos programas desenvolvidos localmente em SEGES deve ser restrito à equipe COTIC. A mesma restrição de acesso aplica-se a bancos de dados, scripts, APIs e demais recursos que sejam utilizados por esses mesmos programas.

5. CONTROLE DE ACESSO FÍSICO

5.1 Deverão ser estabelecidos mecanismos de proteção para as instalações físicas onde se encontram os recursos de TIC e também para as áreas de processamento das informações, prevenindo o acesso físico não autorizado, danos ou interferências.

5.1.1 Poderão ser adotados procedimentos específicos dispondo sobre o acesso físico dos usuários às dependências da SEGES.

5.1.2 Todos os envolvidos em trabalhos de apoio, tais como segurança patrimonial, manutenção das instalações físicas e serviços de conservação e limpeza, devem ser orientados e capacitados para manter as medidas de proteção de acesso adotadas por SEGES.

5.1.3 Não são permitidos registros fotográficos, de imagens, filmagens ou captura de sons no ambiente corporativo da SEGES, salvo quando houver autorização prévia por parte da mesma.

5.1.4 São vedados a divulgação e o compartilhamento do conteúdo de que trata o título 5.1.3 deste manual em mídias sociais, internet ou outros meios eletrônicos, exceto quando autorizados pela área de Comunicação da SEGES.

6. ACESSO REMOTO AOS RECURSOS DE TIC

6.1 As recomendações para acesso aos sistemas e recursos de TIC internos de SEGES, assim como o acesso à rede corporativa de SEGES, para o servidor que esteja trabalhando em área externa à PMSP, ou para qualquer usuário autorizado que necessite realizar algum tipo de acesso remoto a esses mesmos sistemas, redes e recursos de TIC, consistem em:

a) Utilização da VPN (Virtual Private Network) – Rede Privada Virtual ou recursos de VDI (Virtual Desktop Infrastructure), Remote Desktop e outros para realizar o acesso ao ambiente tecnológico corporativo. Exceção feita aos recursos corporativos disponibilizados em ambiente seguro na internet.

b) Utilização das ferramentas de comunicação corporativas: (e-mail corporativo, ferramentas homologadas pela COTIC, para comunicação e compartilhamento de arquivos).

c) Garantia da centralização e do armazenamento das informações corporativas apenas nos servidores corporativos.

d) Garantia de que a estrutura de backup atenda aos critérios de segurança da informação: Integridade, Disponibilidade e Confidencialidade.

e) Criptografia de todas as informações críticas da Secretaria Municipal de Gestão, garantindo que o armazenamento, uso e tráfego destas informações também estejam criptografados.

6.2 Em paralelo ao estabelecido nas recomendações do título 8.1 deste manual, a política de segurança da informação estabelece o que não é recomendável na situação de uso dos recursos de TIC da SEGES em ambiente externo:

a) Exigência de bloqueios, remoção, alterações e/ou instalações no equipamento particular do servidor. Exceção feita aos requisitos mínimos solicitados para a implementação da modalidade de teletrabalho (sistema operacional atualizado, antivírus instalado, etc.)

b) Realização de acesso remoto no equipamento particular, sem solicitar a autorização do servidor.

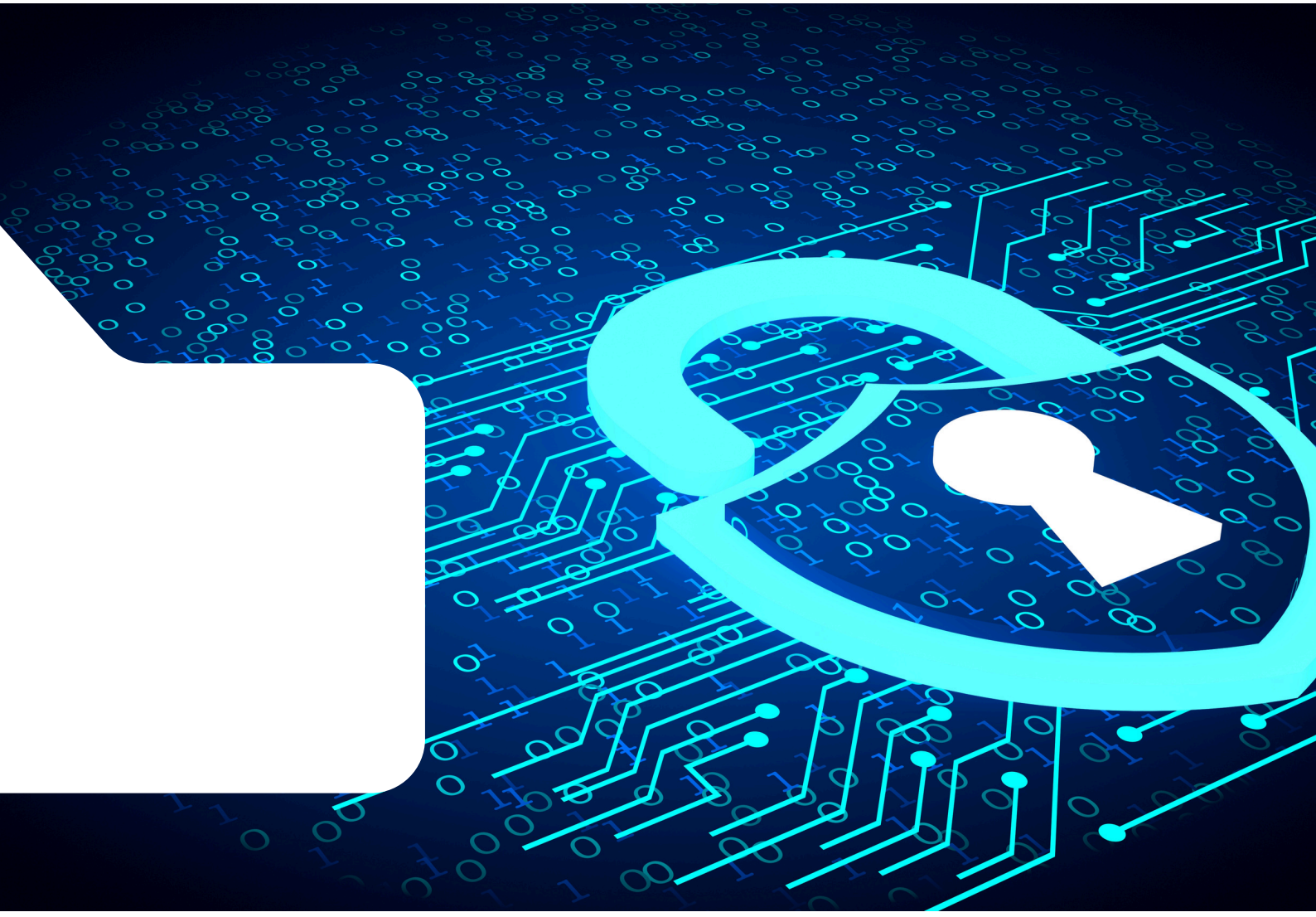
c) Criação de regras e controles que possam gerar conflitos e/ou divergências com leis e regulamentos vigentes.

d) Utilização de credencial de acesso (login – usuário e senha) genérica ou compartilhada para os acessos remotos.

e) Utilização de aplicativos, sistemas e recursos novos não homologados pela COTIC.

7. AVERIGUAÇÃO DE INCIDENTES

As infrações e violações às normas dispostas neste manual de controle de acessos serão inicialmente averiguadas pela COTIC e, a depender da gravidade do caso, poderão ser encaminhadas ao Gabinete da SEGES, para que este tome as medidas cabíveis.



8. DISPOSIÇÕES FINAIS

8.1 Este manual de controle de acessos poderá nortear instrumentos normativos complementares que eventualmente se façam necessários, e que deverão manter a coesão com o conteúdo deste manual de controle de acessos.

8.2 Eventuais exceções às determinações constantes deste manual de controle de acessos serão analisadas individualmente, aplicadas somente ao caso concreto, dentro dos limites e motivos que as fundamentaram.

8.3 O presente manual de controle de acessos poderá ser revisto e atualizado sempre que necessário.

PREFEITURA DE
SÃO PAULO