PREFEITURA DE SÃO PAULO GESTÃO

PSI – Política de Segurança da Informação

Documento de Diretrizes e Normas Administrativas

Secretaria Municipal de Gestão – SG

São Paulo

2018

Histórico de Versões

Versão	Data	Comentários	Autor	Revisor
1.0	05/11/2018		Rafael da Matta	

Sumário

PSI – Política de Segurança da Informação

Objetivo

A PSI - Política de Segurança da Informação é o documento que orienta e estabelece as diretrizes corporativas para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as unidades da Secretaria Municipal de Gestão -SG. Este documento esta baseado em Definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento. Preservar as informações quanto à: Integridade, Confiabilidade e Disponibilidade.

1. Aplicações

Todos os Servidores Públicos, estagiários, terceiros e quaisquer outros usuários devem observar e seguir seus padrões e recomendações.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da PMSP poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada colaborador manter-se atualizado em relação aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

2. Requisitos

Para a uniformidade da informação, esta norma deverá ser comunicada a todos os colaboradores da SG a fim de que a política seja cumprida dentro e fora da empresa.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao Suporte Técnico.

Deverão ser criados e instituídos controles apropriados, registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas desenvolvidos por Secretaria Municipal de Gestão ou por terceiros.

Cabe a~~A~~ Secretaria Municipal de Gestão - SG apurar fatos e responsabilizar ~~exonera-se de toda e qualquer responsabilidade~~o servidor quanto ao ~~decorrente do~~ uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta PSI será implementada por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função, bem como de vínculo ou prestação de serviço.

O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da SG~~instituição~~ e sujeitará o usuário às medidas administrativas e legais cabíveis.

3. Das Responsabilidades

DOS GESTORES DE PESSOAS E/OU PROCESSOS

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da Secretaria Municipal de Gestão - SG.

Exigir dos colaboradores a assinatura no documento sistema eletrônico de processos, referente ao Termo de Compromisso e Condições de Uso, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- Os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.
- Os usuários (logins) de estagiários/terceiros serão de responsabilidade do gestor da área contratante.

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da empresa.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento, licença, transferência entre Secretarias, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Secretaria Municipal de Gestão.

DOS USUARIOS

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

- A senha de acesso obtida por meio do cadastro é pessoal e intransferível, sendo o usuário o único responsável por qualquer ato, legal ou ilegal, decorrente do uso da rede a partir de seu login e senha.
- Não se fazer passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais;
- Zelar pelo uso adequado dos recursos computacionais oferecidos pela Secretaria Municipal de Gestão (SG) em qualquer circunstância;
- Responder pelo mau uso dos recursos computacionais ou por atos que violem as regras aqui descritas.
- Respeitar a privacidade, a confidencialidade e a integridade das informações da PMSP e de outros usuários;
- Evitar comer, fumar ou beber próximo da estação de trabalho;
- Se responsabilizar pelo backup e guarda das informações armazenadas na estação de trabalho que utiliza;
- Reportar qualquer incidente de segurança à área de tecnologia;

- Manter em sua estação de trabalho somente os softwares homologados pela área de tecnologia;
- Utilizar as impressoras de forma consciente;

4. Expressamente Proibido

É expressamente proibido utilizar o serviço para:

- Mostrar, armazenar ou transmitir textos, imagens ou sons que possam ser considerados ofensivos ou abusivos;
- Instigar, ameaçar, ofender, abalar a imagem, invadir a privacidade e/ou prejudicar outros usuários da internet;
- Acessar sites com conteúdo relacionado a sexo, drogas, pornografia, pedofilia, violência ou armamento, conforme o disposto na Lei Municipal nº 14.098/05 e art. 1º do Decreto Municipal nº 49.914/08;
- Acessar sites com conteúdo relacionado a jogos on-line, bate-papo (chats), relacionamento pessoal ou quaisquer outros que não tenham relação com suas atribuições, responsabilidades, atividades e/ou similares;
- Acessar ou tentar acessar recursos computacionais não autorizados previamente pela Secretaria Municipal de Gestão ou de terceiros;
- Usar ou tentar usar a rede para trafegar informações confidenciais e/ou sigilosas de responsabilidade da Secretaria Municipal de Gestão;
- Interceptar ou tentar interceptar a transmissão de dados através de ferramentas de monitoração ou outros métodos;
- Violar ou tentar violar sistemas de segurança, inclusive usando ou tentando usar a identidade eletrônica de outro usuário, senhas ou outros;
- Provocar interferência nos serviços prestados a outros usuários, ou seu bloqueio, principalmente se feito através de congestionamento na rede de dados ou inserção de vírus e/ou worms;
- Causar ou tentar causar a indisponibilidade dos serviços e/ou destruição de dados ou engajar-se em ações que possam ser consideradas como de violação da segurança computacional.
- Fins políticos ou comerciais, tais como envio de mala direta ou propaganda política;
- Obter ganho ou vantagem indevida e/ou vedada por lei.
- Intimidar, difamar, assediar ou, de qualquer forma, aborrecer outras pessoas;

- Consumir inutilmente os recursos computacionais da PMSP, com objetivos diversos daqueles relacionados às suas atribuições, responsabilidades e atividades.
- Conectar notebook pessoal na rede cabeada coorporativa.

5. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta PSI a Secretaria Municipal de Gestão poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônicas, conexões com a internet, dispositivas móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria;
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

6. Correio Eletrônico

Serviço de Correio Eletrônico Corporativo, utilizado para comunicação entre órgãos da administração pública direta e indireta da Prefeitura de São Paulo (PMSP), são esses: Transmissão de mensagens eletrônicas (elaborar, enviar, encaminhar, responder, arquivar, copiar, ler ou imprimir); Assistente de ausência temporária; Redirecionamento de mensagens; Criação de regras para recepção, arquivamento ou deleção de mensagens; Lista de usuários cadastrados na rede corporativa PMSP; Aviso de consumo da caixa postal; Acesso via Webmail; Recuperação das mensagens apagadas dos últimos 30 dias; Acesso via dispositivos móveis, (ActiveSync, programa da Microsoft para sincronização entre PCs e dispositivos moveis).

7. Internet

As regras estabelecidas visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da Secretaria, que pode analisar e, se necessário, bloquear qualquer arquivo, site,

correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor.

Somente os colaboradores que estão devidamente autorizados a falar em nome da Secretaria Municipal de Gestão para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela área de tecnologia.

Os colaboradores não poderão em hipótese alguma utilizar os recursos da PMSP para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

A utilização de ferramenta especifica (Youtube, Facebook, etc…) poderão ser utilizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Para tal, grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos gestores, precisam ser criados a fim de viabilizar esse acesso especial. Mediante solicitação e aprovação da área técnica responsável, o uso será passível de concessão, em regime de exceção, quando eles tiverem natureza intrínseca às atividades relacionadas.

O acesso à rede sem fio é permitido somente aos visitantes e servidores devidamente cadastrados, doravante denominados “usuário” ou “usuários”. Para sua utilização, deve manter seus computadores pessoais, celulares e tablets com softwares (patches, errata) e antivírus atualizados, conforme orientação do administrador de rede.

Ao utilizar a rede sem fio para acesso à Internet, o interessado expressamente aceita, sem reservas ou ressalvas, todas as condições aqui descritas para a utilização do serviço.

A Secretaria Municipal de Gestão não tem obrigação de controlar, e não controla, o conteúdo e natureza dos conteúdos transmitidos, difundidos ou postos a disposição de terceiros através da rede sem fio; não obstante, se reserva o direito de revisar, a qualquer momento e sem aviso prévio, por iniciativa própria ou a pedido de terceiro, os conteúdos transmitidos, difundidos ou postos à disposição de terceiros pelos usuários.

A Secretaria Municipal de Gestão se reserva o direito de cancelar ou suspender o serviço sem prévio aviso aos usuários

8. Acesso a Rede Corporativa

A criação do usuário de rede (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.

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese. Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante SG e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação da chefia de uso compartilhado ele deverá ser responsabilizado.

Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha, conforme orientações:

- A senha precisa ter no mínimo 8 (oito) caracteres.
- A senha precisa ter caracteres maiúsculos, minúsculos, números e se possível caracteres especiais (por exemplo: \!\@\#\$\%\¨).
- A senha não pode conter parte do nome ou sobrenome do usuário.
- Quando o usuário efetuar login na estação de trabalho deve ser escolhido o domínio REDE.
- Não pode ser utilizado as últimas 24 (vinte e quatro) senhas.
- A senha deve ser alterada a cada 60 (sessenta) dias.
- A senha pode ser alterada novamente após 2 (dois) dias.
- Após 6 (seis) tentativas incorretas da senha, sua conta é bloqueada automaticamente por 5 (cinco) minutos. Após esse tempo, tente o acesso novamente na sua estação de trabalho.
- A senha deve ser alterada em todos os dispositivos móveis.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

9. Equipamentos de TI

Os equipamentos disponibilizados aos colaboradores são de propriedade da PMSP, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da Secretaria.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da área de tecnologia, ou de quem este determinar. As Coordenadorias que necessitarem fazer testes deverão solicitá-los previamente à área de tecnologia, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Os sistemas e computadores devem ter versões do software antivírus instalados, ativados e atualizados permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no SCD – Sistema Central de Demandas (http://smgsuporte.prefeitura.sp.gov.br).

Documentos imprescindíveis para as atividades dos colaboradores deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os colaboradores detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da área de tecnologia.

10. Do Ato Proposital de Violação

Considera-se violação das regras:

- Infringir qualquer lei ou regulamento local, estadual, nacional ou internacional aplicável;
- Desrespeitar quaisquer das proibições constantes neste Termo de Responsabilidade.
- Não observar os deveres instituídos nesta política de uso.

O descumprimento de qualquer regra constante nesta PSI sujeitará o usuário infrator às seguintes penalidades: advertência formal; suspensão do acesso pelo período de até 30 (trinta) dias, à critério da Secretaria Municipal de Gestão; proibição permanente do uso do serviço, em caso de reincidência.

As penalidades acima estabelecidas serão aplicadas sem prejuízo da responsabilidade civil, criminal e/ou funcional do usuário;

Caso alguma violação seja verificada pelo sistema de monitoramento, será bloqueado o acesso do usuário infrator à rede, sendo ele a seguir notificado do ocorrido por meio do e-mail de contato constante de seu cadastro.

11. Disposições Gerais

A Secretaria Municipal de Gestão se reserva o direito de suspender o acesso do usuário que estiver descumprindo quaisquer das regras constantes na presente PSI, inclusive por consumo excessivo.

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da Secretaria Municipal de Gestão. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

ANEXO I – TERMO DE COMPROMISSO E CONDIÇÕES DE USO

Este termo de compromisso aplica-se a todos os usuários da Secretaria Municipal de Gestão de São Paulo e suas Unidades.

Termo de Compromisso para Usuários

Declaro que li e estou de acordo com o Manual de Padrões e Recomendações de Usuários, tendo compreendido todo o seu conteúdo.

Declaro, ainda, estar ciente de que violações a política de segurança resultarão em medidas disciplinares administrativas, ou outras medidas pertinentes por parte da SG.

São Paulo, ____ de _____de _____.

_____

Nome

Orgão