Anexo I

Política de Segurança da Informação

Documento de Diretrizes e Normas Administrativas

Secretaria Municipal de Planejamento e Assuntos Estratégicos
Coordenação de Planejamento e Gestão de Tecnologia da Informação e Comunicação
(SMPAE – CGTI)

Versão 1.0

Última atualização 09 de Fevereiro de 2023

Sumário

Introdução

A informação é um recurso fundamental para o desenvolvimento das atividades de qualquer organização, e como tal, necessita ser protegida. A **Política de Segurança da Informação (PSI)** visa preservar seus princípios básicos, que são a disponibilidade, a integridade e a confidencialidade.

Este documento reúne diretrizes e normas acerca da **Segurança da Informação (SI)**, com o objetivo de minimizar riscos de perdas ou violação de qualquer ativo de TI. A **PSI** se aplica a todos os Servidores Públicos, Secretarias, Órgãos, Fornecedores, Prestadores de Serviço e demais parceiros vinculados a Prefeitura Municipal de Porto Alegre (**PMPA**).

Em agosto de 2018 foi aprovada a Lei 13709**,** ou Lei Geral de Proteção de Dados **(LGPD)**, que entrou em vigor em setembro de 2020, mas passou a ter vigência plena em agosto de 2021. A lei visa regulamentar a coleta e a utilização de dados pelas empresas e organizações para garantir o correto tratamento e a privacidade de dados pessoais de posse destas. De acordo com a **LGPD**, as empresas e organizações não podem mais tratar dados pessoais sem autorização e, em caso de incidente de segurança de dados pessoais, devem avisar a todas as pessoas impactadas, bem como a **Autoridade Nacional de Proteção de Dados** (ANPD).

De acordo com a **LGPD**, dado pessoal é todo aquele que identifica um indivíduo, este que é o **titular dos dados;** como nome, RG, CPF, endereço, telefone, e-mail etc. São ainda inclusos, na legislação, todo dado sensível, que inclui informações sobre religião, saúde, etnia, biometria, posicionamento político ou qualquer dado que possa deixar o indivíduo mais vulnerável à discriminação de qualquer ordem. A **LGPD** define uma série de obrigações por parte das organizações que fazem o **tratamento de dados**, que são as operações realizadas com os dados pessoais do **titular dos dados**, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, transferência, difusão ou extração.

A Prefeitura Municipal de Porto Alegre é o **controlador** dos dados tratados na realização das suas atividades legais e constitucionais. Os **operadores** são responsáveis por tratar dados pessoais, na prática, conforme determinações estabelecidas pelo **controlador**. O **encarregado** ou **DPO** *(Data Protection Officer)* é a pessoa indicada pelo **controlador** e **operador** para aceitar reclamações e comunicações dos titulares, prestar esclarecimentos, adotar providências, tratar

com a **Autoridade Nacional de Proteção de Dados** (ANPD), orientar a respeito das práticas a serem tomadas em relação à proteção de dados pessoais e executar as demais atribuições determinadas pelo **controlador** ou estabelecidas em normas complementares.

Ao servidor municipal não é dado o direito de desconhecimento desta **PSI** devendo seguir rigorosamente o disposto em suas normas e diretrizes. Para isso, a presente **PSI** deve ser comunicada para todo o pessoal envolvido e largamente divulgada a partir da data de sua entrada em vigor.

A inobservância das diretrizes e normas de segurança desta **PSI** sujeita o usuário a sanções administrativas e, em casos mais graves, às leis vigentes.

1. Objetivos

1.1. A Política de Segurança da Informação (**PSI)** tem como objetivos:

1.1.1. Estabelecer orientações e diretrizes que assegurem a segurança das informações em meio físico e digital;

1.1.2. Nortear a definição de normas e diretrizes específicas de **SI**, bem como a implementação de controles e processos para seu atendimento.

1.2. Os objetivos supracitados visam garantir os seguintes princípios básicos da informação:

- **Disponibilidade**: É a certeza de que a informação estará acessível e disponível em escala contínua para as pessoas autorizadas. Atualmente os mecanismos de acesso remoto tornam possível a disponibilidade da informação. Mecanismos de autenticação, canais de acesso e sistemas devem funcionar corretamente para garantir que os dados e informações estejam disponíveis de qualquer lugar em que o usuário esteja e a qualquer hora. O desempenho de qualquer organização é prejudicado se dispositivos, sistemas, aplicativos e dados não puderem ser acessados.

- **Integridade**: É a garantia de que a informação estará completa, exata e preservada contra alterações indevidas, fraudes ou até mesmo contra a sua destruição, assim evitando violações da informação, sejam estas de forma acidental ou mesmo proposital. Garantir a integridade é adotar as precauções necessárias para que a informação não seja modificada ou eliminada sem autorização. Ou seja, é necessário manter a sua legitimidade e consistência, condizendo exatamente com a realidade.

- **Confidencialidade**: A informação só pode ser acessada e atualizada por pessoas autorizadas e devidamente credenciadas. Dados e informações importantes de alguns setores ou clientes jamais podem ser acessados por terceiros estranhos à corporação. Devem haver mecanismos de segurança de Tecnologia da Informação (TI) capazes de impedir que pessoas não autorizadas acessem informações sigilosas, seja por engano ou por má-fé. Os dados pessoais contidos nas Informações devem ser tratados com a adoção de medidas técnicas e organizacionais de **SI**, nos termos impostos pela **LGPD** e normativos municipais referentes à matéria.

1.3. É importante lembrar que **SI** não está ligada somente a prevenção de ataques cibernéticos, realizados por criminosos que infectam dispositivos na rede corporativa, mas fortemente a implementação de controles e práticas para aprimorar a postura de segurança como um todo.

2. Abrangência

2.1. A **SI** e a sua classificação abrangem aspectos físicos, tecnológicos e humanos, e orientam-se pelos princípios da Disponibilidade, Integridade e Confidencialidade.

2.2. Esta **PSI** se aplica a todos os servidores públicos, secretarias, órgãos, fornecedores, prestadores de serviço e demais parceiros vinculados a Prefeitura Municipal de Porto Alegre (**PMPA**), independente da modalidade de trabalho exercida (presencial ou teletrabalho).

2.3. As medidas de proteção devem ser adotadas durante todo o ciclo de vida e tratamento da informação (coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, transferência, difusão ou extração).

3. Responsabilidades dos Servidores Municipais da PMPA

Todos os Servidores da **PMPA** devem seguir o disposto nesta **PSI** e suas normas**,** compreendendo seu propósito e a classificação das informações. Como fonte de informações complementares, disponibilizamos orientações através do Guia de Boas Práticas de Segurança da Informação.

3.1. Acesso à Rede e Utilização dos Recursos Computacionais

3.1.1. O acesso à rede e a utilização de recursos, provida pela PMPA aos servidores públicos municipais (usuários), está condicionado à observância a presente **Política de Segurança da Informação (PSI)**.

3.2. Informação

3.2.1. O tratamento de dados pessoais está restrito apenas as atividades de interesse da PMPA ou órgãos vinculados, de acordo com a LGPD e demais leis vigentes elencadas ao final deste documento no tópico - Leis e Normativos Referencias.

3.2.2. Usuários que venham a ter acesso a informações sigilosas e/ou proprietárias deverão ter atenção ao expresso na **cláusula 7 - Confidencialidade e Propriedade Intelectual** deste documento.

3.2.3. É expressamente proibido o uso de qualquer recurso corporativo para prática de ato ilícito, sob pena de responsabilização civil ou criminal.

3.2.4. Cabe ao usuário manter as informações de sua responsabilidade sempre atualizadas e com cópia de segurança, conforme descrito na Norma para Procedimentos de Backup. Desta forma evitando eventual perda de informações por serem mantidas localmente apenas.

3.3. Credenciais

3.3.1. A credencial de acesso aos recursos computacionais da **PMPA,** por padrão será restritiva, provendo acesso somente aos equipamentos de informática e *software* relevantes para o desempenho das suas atividades funcionais, conforme perfil básico definido.

3.3.2. A credencial de acesso aos recursos computacionais da **PMPA** é de inteira responsabilidade do usuário, pessoal e intransferível, e não deverá, em hipótese alguma, ser compartilhada ou fornecida a outros servidores municipais ou terceiros.

3.3.3. É responsabilidade do usuário conhecer e seguir as orientações de uso de credenciais e criação de senhas reunidas na Norma para Utilização De Credencias e Senhas.

3.4. Acesso à internet

3.4.1. O acesso à internet deverá ser utilizado primariamente para o desempenho das atribuições funcionais, sendo admitido o uso eventual da internet, por curtos períodos, para fins pessoais, desde que tal uso não comprometa o desempenho, pelo usuário, das suas atribuições funcionais e desde que esteja em conformidade com os demais termos desta **PSI**.

3.4.2. Considera-se transgressão grave a esta **PSI** o acesso feito pelo usuário a *sites* que façam apologia, incitem ou facilitem atividades criminosas, com conteúdo pornográfico, racista, jogos de apostas ou que tragam aos equipamentos e à rede códigos maliciosos, artifícios de violação ou quaisquer outros elementos que possam vir a alterar ou danificar a rede, os equipamentos, os sistemas e os bancos de dados da **PMPA**, ou ainda cujo conteúdo possa denegrir a imagem da **PMPA** ou órgãos vinculados.

3.4.3. Deve ser de conhecimento dos usuários que todos os seus acessos a *sites* na internet podem ser monitorados. Em caso de dúvida, deve-se verificar junto aos superiores se determinado *site* pode ser acessado.

3.4.4. Não é permitido o *download,* envio ou hospedagem de músicas, filmes, vídeos, jogos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura local ou que violem as leis de direitos autorais.

3.4.5. Tentativas de contornar controles corporativos (como acesso à rede usando proxies anônimos) serão vistas como violação de conduta e infração funcional.

3.5. Acesso ao Correio Eletrônico e Mensageria

3.5.1. Os usuários deverão utilizar o correio eletrônico (e-mail) e os serviços de mensageria (mensagens instantâneas) disponibilizados pela **PMPA** como meios de receber e enviar comunicações oficiais e informações relacionadas às atividades funcionais.

3.5.2. Os serviços de e-mail e mensageria fornecidos ao usuário são propriedade da **PMPA.** As informações contidas nas mensagens eletrônicas podem ser monitoradas a qualquer tempo, sem aviso ou notificação prévia, para fins de auditoria de conformidade a esta **PSI**.

3.5.3. O usuário deverá seguir a Norma para Uso de E-Mails e Mensageria, sendo responsável pela correta utilização do recurso, bem como pelo conteúdo das transmissões feitas através do correio eletrônico a partir de sua credencial.

3.6. Equipamentos de Informática e Softwares

3.6.1. Os equipamentos de informática disponibilizados pela **PMPA** deverão ser utilizados somente para o desempenho das atribuições funcionais.

3.6.2. Recursos computacionais conectados a rede da **PMPA** devem estar em conformidade aos padrões de segurança homologados com o Fornecedor de TI responsável, devendo o usuário zelar pela integridade dos equipamentos, mantendo-os limpos e em boas condições conforme a Norma para Uso de Equipamentos e Software.

3.6.3. Fica proibida a utilização de equipamentos próprios do usuário na rede corporativa (domínio do AD) da **PMPA**. O uso dos equipamentos particulares está limitado por padrão à rede *wireless* “Porto Alegre Livre”, ou rede visitante equivalente que esteja logicamente isolada da rede disponibilizada pela **PMPA**.

3.6.4. Quando da necessidade de acesso remoto à rede da **PMPA** via VPN, para o teletrabalho autorizado pelas chefias, este deverá ser concedido e utilizado de acordo com o Manual de Instalação e Orientações para Uso da VPN.

3.6.5. Os usuários devem fazer uso racional dos recursos de tecnologia da informação disponíveis, priorizando o interesse público e institucional.

4. Responsabilidades dos Gestores de Pessoas e/ou Processos

4.1. Além do cumprimento do exposto no item anterior, que elenca as responsabilidades dos servidores**,** é esperado que os gestores mantenham postura exemplar em relação à **SI**, servindo como modelo de conduta para os servidores municipais sob a sua gestão, devendo levar a estes o conhecimento sobre a **PSI** e cobrar seu integral cumprimento.

4.2. Gestores devem informar imediatamente, através dos canais estabelecidos pela **PMPA**, todos os casos de encerramento de vínculo funcional, alteração ou afastamento de seus subordinados, de maneira que as suas credenciais de rede sejam excluídas ou alteradas pelos responsáveis de TI, com a celeridade apropriada.

4.3. Gestores devem Informar imediatamente, através dos canais estabelecidos pela **PMPA**, quaisquer situações de desaparecimento de dispositivos e equipamentos de TI, de forma que seja procedida a devida busca, sindicância e baixa, conforme o caso.

5. Responsabilidades da Área de Tecnologia da Informação

5.1. Compõe a Área de Tecnologia de Informação todos os setores designados pela **PMPA**, bem como fornecedores e prestadores de serviços de TI contratados para o cumprimento de suas atividades competentes de acordo com o presente item.

5.2. Cabe aos fornecedores e prestadores de serviços de TI contratados adequarem todos os seus serviços a esta **PSI**, normativos e leis vigentes, bem como a quaisquer outras pertinentes aos interesses da **PMPA** que possam entrar em vigor pelos canais oficiais da **PMPA**.

5.3. Os fornecedores e prestadores de TI devem estar em conformidade com a Lei 13709 - Lei Geral de Proteção de Dados (**LGPD**), mantendo acessível em sítio (*website*) de acesso público, ou conforme requisitado, suas políticas e esclarecimentos relacionados ao tema.

5.4. Fica a Área de Tecnologia de Informação obrigada a seguir as orientações e diretrizes contidas na Norma para Padrões de Segurança de Informação.

6. Classificação da Informação

6.1. As informações serão classificadas de acordo com a confidencialidade e as proteções necessárias, conforme descritos na Norma para Classificação da Informação.

6.2. Na classificação da informação devem se consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

7. Confidencialidade e Propriedade Intelectual

7.1. Manter sigilo, tanto escrito como verbal, ou, por qualquer outra forma, de todos os dados, informações científicas e técnicas e, sobre todos os materiais obtidos com sua participação, podendo incluir, mas não se limitando a: técnicas, desenhos, cópias, diagramas, modelos, fluxogramas, croquis, fotografias, programas de computador, discos, pen drives, processos, projetos, dentre outros.

7.2. Não revelar, reproduzir, utilizar ou dar conhecimento, em hipótese alguma, a terceiros, de dados, informações científicas ou materiais obtidos com sua participação, sem a prévia análise da PMPA sobre a possibilidade de proteção, nos órgãos especializados, dos resultados ou tecnologia envolvendo aquela informação.

7.3. Não tomar, sem autorização da PMPA, qualquer medida com vistas a obter para si ou para terceiros, os direitos de propriedade intelectual relativos às informações a que tenha acesso.

7.4. A comprovada violação de confidencialidade e/ou de propriedade intelectual acarretará na aplicação das medidas disciplinares cabíveis, além de eventual indenização e ressarcimento à PMPA, quando aplicável, pelas perdas, danos diretos e indiretos e quaisquer outros prejuízos patrimoniais ou morais que surjam em decorrência desta violação.

8. Medidas Disciplinares

8.1. As violações a esta **PSI** estão sujeitas às sanções disciplinares previstas, nas normas internas da **PMPA** (Artigo 203 da Lei Complementar 133/85, Porto Alegre) e na legislação vigente no Brasil.

8.2. O descumprimento das disposições constantes na **PSI** caracteriza infração funcional ou contratual, conforme o caso, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades legais cabíveis.

8.3. Não será permitido o descumprimento das diretrizes e normas da PSI pela alegação de desconhecimento das mesmas por parte do agente envolvido.

8.4. O uso indevido, ou não autorizado, dos recursos de Tecnologia da Informação, bem como qualquer ação em desacordo com os termos desta **PSI** sujeitarão o infrator à aplicação das penalidades previstas na legislação e nos regulamentos internos da **PMPA**, sem prejuízo das responsabilidades legais cabíveis.

9. Divulgação

A **PSI** e suas normas complementares serão amplamente divulgadas a todos os Servidores Públicos, fornecedores e prestadores de serviços vinculados à **PMPA**, bem como terá acesso disponibilizado nos canais de comunicação.

10. Vigência e Periodicidade de Revisão

A **PSI** será revisada a cada 4 (quatro) anos e as normas complementares a cada 12 (doze) meses. Revisões também podem ocorrer por força de eventos relevantes como mudanças na legislação, de atualizações tecnológicas que impactem a segurança ou aperfeiçoamento desta **PSI**.

11. Considerações Finais

11.1. O descumprimento dos preceitos deste documento ou de outros relacionados pode acarretar medidas disciplinares, medidas administrativas ou judiciais cabíveis, podendo levar a sansões administrativas, inclusive decorrentes da legislação, autorregulação ou regulamentação aplicável, não sendo aceitável a alegação de desconhecimento.

11.2. A **PMPA** e órgãos vinculados se reservam ao direito de monitorar todas as atividades feitas pelos seus usuários em seus sistemas de informação para garantir o cumprimento desta e outras políticas.

12. Leis e Normativos Referencias

Lei 12965 – Marco Civil Internet – Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Lei 12527 – Lei do Acesso a Informação (LAI). Dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir 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.

Lei 13460 - Estabelece normas básicas para participação, proteção e defesa dos direitos do usuário dos serviços públicos prestados direta ou indiretamente pela administração pública.

Lei 13709 - Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019) . Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Lei 9609 - Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País e dá outras providências.

LC 133 - Lei Complementar Nº 133, de 31 de Dezembro de 1985. Estabelece o estatuto dos funcionários públicos do município de porto alegre.

OS 007/2018 – Regulamenta e uniformiza a utilização dos recursos de Tecnologia da Informação e Comunicação (TIC) no âmbito da Administração Municipal.

Normas Complementares

Norma para Classificação de Informação

Norma para Credenciais e Senhas

Norma para Padrões de Segurança da Informação

Norma para Plano de Resposta de Incidentes

Norma para Procedimentos de Backup

Norma para Repositório Oficial de Arquivos

Norma para Uso de e-mails e Mensageria

Norma para Uso de Equipamentos e Software

Versão	Data	Alterações	Autor	Revisor
1.0	09/02/2023	Versão inicial	(CGTI-SMPAE) Eduardo Hoppe Fernando Delazeri Jefferson Bregalda Vanessa Schmitz	(CGTI-SMPAE) Eduardo Hoppe