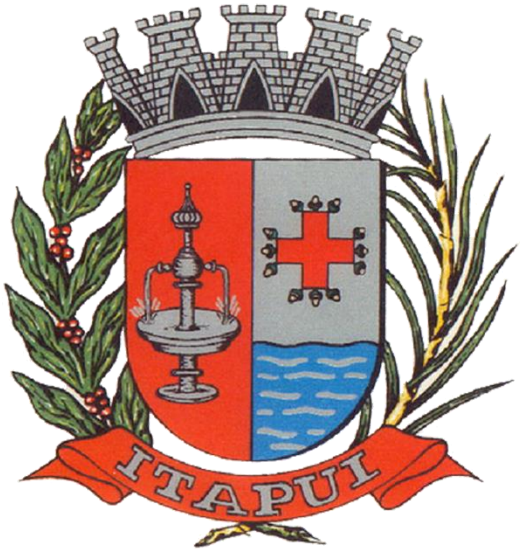
# PSI
# 2021-2022




PREFEITURA DE
ITAPUÍ

## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

# Sumário

# Referências legais e normativas

ABNT ISO GUIA 73:2009 – Gestão de riscos – Vocabulário – Definições de termos genéricos relativos à gestão de riscos.

ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos.

ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação.

Lei nº 12.965, de 23 de abril de 2014 (“Marco Civil da Internet”) - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Este documento se aplica no âmbito da Prefeitura Municipal de Itapuí.

- **Objetivo Geral**

  Estabelecer direcionamentos e valores para a gestão da segurança da informação no âmbito da Prefeitura Municipal de Itapuí.
- **Descrição e Escopo**

  Este documento contém princípios e diretrizes aplicáveis à segurança das informações custodiadas ou de propriedade da Prefeitura Municipal de Itapuí, estabelecendo direcionamentos e valores para a gestão da segurança da informação.
- **Público-alvo**

  Este documento se destina a todos os colaboradores ativos e inativos da Prefeitura Municipal de Itapuí, sejam eles servidores públicos efetivos, seletivos ou comissionados, estagiários, prestadores de serviço, visitantes ou usuários externos do sistema de informação da Prefeitura, sendo de responsabilidade de cada um o seu cumprimento.

# 1. SIGLAS, TERMOS E DEFINIÇÕES

**Ação de evitar o risco** - Decisão de não se envolver ou agir de forma a se retirar de uma situação de risco (NBR ISO/IEC 27005, 2008).

**Aceitar/Reter o risco** - Aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco (NBR ISO/IEC 27005, 2008).

**Ameaça** - Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou uma organização (ISO/IEC 27000, 2014).

**Ativo** - Qualquer elemento que tenha valor para a organização (NBR ISO/IEC 27002, 2005).

**Ativos Críticos de Tecnologia da Informação** - São os Ativos de Tecnologia da Informação indispensáveis aos processos diretamente relacionados aos objetivos estratégicos da Instituição.

**Ativo de Informação** - Dados, informações e conhecimentos obtidos, gerados, tratados e/ou armazenados, como por exemplos base de dados, arquivos, contratos, acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos e planos institucionais, processos de trabalho, entre outros.

**Ativo de Tecnologia da Informação** - Composto por ativos de *software* e ativos físicos, permitindo o armazenamento, a transmissão e processamento das informações. Exemplos de ativos de *software*: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários. Exemplos de ativos físicos: os equipamentos computacionais fixos e móveis, equipamentos utilizados na Política de Segurança da Informação e Comunicações para comunicação de dados e mídias removíveis.

***Backup*** - Cópias de segurança de arquivos (NBR ISO/IEC 27002, 2005).

**Conformidade** - Estar de acordo com determinadas normas, regras ou preceitos.

**Contas de Serviço** - Contas de acesso à rede corporativa de computadores necessários a um procedimento automático (aplicação, *script* etc.), sem qualquer intervenção humana no seu uso.

**Controle de Acesso** - Conjunto de procedimentos, recursos e meios utilizados com a finalidade de garantir que os acessos aos ativos só ocorrerão após autorização e serão restritos, baseados nos requisitos de segurança e nas atividades do usuário (ISO/IEC 27000, 2014).

**Credenciais ou Contas de Acesso** - Identificação única, concedida de forma pessoal e intransferível a uma pessoa, em conjunto com um método de autenticação. Esse par de informações habilita o seu dono a acessar equipamentos, sistemas e aplicações específicas, de acordo com o perfil definido.

**Classificação da Informação** - Identificação do nível de proteção requerido pela informação, atribuído por autoridade competente.

**Confidencialidade** - Nenhuma informação estará disponível ou será divulgada a entidades (pessoas, sistemas ou órgãos) não autorizadas.

**Colaborador** - Servidores públicos efetivos, contratados por tempo determinado ou comissionados; estagiários; prestadores de serviço; visitantes; ou, ainda, quaisquer usuários externos do sistema de informação da Prefeitura Municipal de Itapuí.

**Criticidade** - Medida de risco obtida da combinação entre o possível impacto na Instituição ou em um projeto e a probabilidade de ocorrência de um evento que os afete.

**Custodiante do Ativo** - Unidade administrativa responsável pelo armazenamento, pela operação, administração e preservação de ativos.

**Custodiante da Informação** - Colaborador responsável pela guarda adequada do dado.

**Divulgação** - Ato de tornar público o resultado de uma informação.

**Equipe de Tratamento de Incidentes** - Grupo de pessoas com a responsabilidade de analisar, tratar e documentar os incidentes de segurança nas redes de computadores, e o tratamento aplicado.

**Gestor** - Unidade administrativa responsável por gerenciar determinado segmento de dados e todos os ativos relacionados.

**Incidente** - Um ou mais eventos indesejados ou inesperados que podem causar algum dano, colocando em risco os ativos de informação, com probabilidade de interromper ou afetar a qualidade dos serviços e/ou atividades da Instituição.

**Infraestrutura de Tecnologia da Informação** - Instalações prediais, equipamentos, computadores, *software*, redes, telecomunicações, sistemas de armazenamento e recuperação de dados, aplicações computacionais, cabeamento e rede telefônica.

**Mitigar/Reduzir o risco** - Efetuar ações que reduzam a probabilidade, consequências negativas, ou ambas, associadas a um risco (NBR ISO/IEC 27005, 2008).

**PDTI** - Plano Diretor de Tecnologia da Informação.

**PMI** - Prefeitura Municipal de Itapuí.

**Política** - Intenções e diretrizes da organização, formalmente expressas pela direção da Instituição (ISO/IEC 27000, 2014).

**PSI** - Política de Segurança da Informação.

**Risco** - Efeito da incerteza sobre os objetivos de segurança da informação associado com o potencial de que as ameaças explorarão vulnerabilidades de um ativo de informação ou grupo de ativos de informação e, assim, causar danos a uma organização (ISO/IEC 27000, 2014).

**Segurança da Informação** - Preservação da confidencialidade, da integridade e da disponibilidade das informações (ISO/IEC 27000, 2014).

**Sigilo** - Confidencialidade, segredo.

**TI** - Tecnologia da Informação.

**Transferir o risco** - Compartilhamento com uma outra entidade do ônus da perda ou do benefício do ganho associado a um risco (NBR ISO/IEC 27005, 2008).

**Vulnerabilidade** - Fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças (ISO/IEC 27000, 2014).

# 2. OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

A Política de Segurança da Informação (PSI) é um documento que estabelece as diretrizes e as normas de segurança que visam a proteger a integridade, disponibilidade, conformidade e autenticidade dos dados e informações de uma Instituição pública ou privada. Consiste num conjunto de ações técnicas e boas práticas relacionadas ao uso seguro de dados. Trata-se de um documento que determina ações importantes para garantir a segurança da informação.

As melhores práticas relacionadas à governança de tecnologia da informação (TI) recomendam a implantação de uma política de segurança como um dos instrumentos para realizar uma gestão eficiente dos recursos da área de TI.

Esta PSI se fundamenta nas recomendações da norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes no país.

**A PSI tem por objetivos específicos:**

2.1 Estabelecer diretrizes que permitam aos colaboradores da Prefeitura Municipal de Itapuí seguirem padrões de comportamento que contribuam com à segurança da informação, preservando as informações quanto à:

**Integridade**: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

**Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

**Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2.2 Desenvolver um comportamento ético/profissional quanto a utilização das ferramentas de TI e as informações por elas geradas visando reduzir ameaças através da adoção de medidas preventivas para evitar possíveis incidentes que podem trazer prejuízos à Prefeitura Municipal de Itapuí.

# 3. PRINCÍPIOS

Este PSI incorpora princípios de Segurança da Informação definidos na Norma ISO/IEC 27000, de 15.01.2014, a saber:

**Atualidade** – As normas e procedimentos devem ser constantemente atualizados, de modo a refletir as mudanças legais, sociais e tecnológicas que interferem na sua aplicabilidade;

**Aplicabilidade** – Os processos de segurança devem ser coordenados e integrados entre si e incorporados nos processos de trabalho e práticas de todas as unidades da Prefeitura Municipal de Itapuí;

**Autenticidade** – Toda informação terá sua origem certificada;

**Clareza** – Todas as normas e procedimentos de segurança produzidos devem ser claros o suficiente para que todos os envolvidos com a informação entendam as suas responsabilidades, bem como os seus direitos e limites;

**Conhecimento** – Os servidores devem ser continuamente capacitados para o desenvolvimento da cultura de segurança da informação;

**Confidencialidade** – Nenhuma informação estará disponível ou será divulgada a entidades (pessoas, sistemas ou órgãos) não autorizadas;

**Disponibilidade** – Toda informação estará disponível e poderá ser utilizada sob demanda por entidade autorizada (pessoa, sistema ou órgão);

**Integridade** – Os ativos de informação deverão ser protegidos, garantindo que só sejam alterados de forma autorizada e não acidental.

# 4. DIRETRIZES

As diretrizes da PSI estão alinhadas com as seguintes diretrizes do Plano Diretor de Tecnologia da Informação (PDTI) da Prefeitura Municipal de Itapuí:

• Promover a governança de TI.

• Promover a melhoria dos sistemas de informação.

• Garantir a segurança da informação e comunicações.

• Manter os processos internos de TI mapeados, formalizados, mensurados e otimizados.

As diretrizes da PSI deverão ser seguidas por todos os colaboradores da Prefeitura Municipal de Itapuí, estejam eles no exercício de suas funções ou não, além de incluir qualquer pessoa, física ou jurídica, que venha a ter acesso a dados ou informações da Prefeitura em qualquer meio ou suporte.

**A PSI tem as seguintes diretrizes:**

4.1 Toda informação gerada pelos colaboradores, utilizando integralmente ou parcialmente recursos da Prefeitura Municipal de Itapuí, é de propriedade do órgão;

4.2 Todos os mecanismos de proteção utilizados para a segurança da informação devem ser mantidos para preservar a continuidade do negócio;

4.3 Ameaças e riscos devem ser reavaliados periodicamente para garantir que a organização esteja efetivamente protegida;

4.4 O acesso às informações, produzidas ou recebidas deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades dos usuários internos;

4.5 Os processos de aquisição ou contratação de bens e serviços de tecnologia da informação devem refletir esta PSI, sem prejuízo da observância da legislação em vigor;

4.6 Os equipamentos de informática e comunicação, bem como os sistemas e as informações deverão ser utilizados para a realização das atividades profissionais;

4.7 Esta política de Segurança da Informação pode ser revisada periodicamente e eventualmente alterada na ocorrência de eventos ou fatos relevantes;

4.8 Os colaboradores devem evitar a circulação das informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso;

4.9 Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e as redes do órgão poderão ser monitorados e gravados conforme previsto nas leis brasileiras;

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

# 5. RESPONSABILIDADES

## 5.1 Colaboradores

5.1.1 É de inteira responsabilidade de cada colaborador todo o prejuízo ou o ressarcimento pelo dano que vier a sofrer ou a causar à Prefeitura Municipal de Itapuí ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

## 5.2 Gestores de Pessoas e/ou Processos

5.2.1 É responsabilidade dos Gestores de Pessoas e/ou Processos manter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

5.2.2 O Gestor é responsável por atribuir aos colaboradores, na fase de contratação, de prestação de serviços ou de efetivação de parceria, a responsabilidade do cumprimento da PSI da Prefeitura Municipal de Itapuí.

5.2.3 O Gestor deve exigir dos colaboradores a assinatura do Termo de Ciência e Compromisso com Cláusula de Confidencialidade (Anexo), assumindo o dever de seguir as normas estabelecidas.

5.2.4 Cabe ao Gestor adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

## 5.3 Setor de Recursos Humanos

5.3.1 Informar ao Setor de Tecnologia da Informação quando houver o desligamento de funcionários, para que as credenciais de acesso aos sistemas, computadores, *e-mail* e ambiente de rede sejam bloqueadas.

## 5.4 Custodiantes da Informação (Área de Tecnologia da Informação)

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

5.4.2 Garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário no caso de movimentação interna dos ativos de TI.

5.4.3 Promover cultura de segurança da informação e comunicações.

5.4.4 Supervisionar, analisar e avaliar a eficácia dos controles de segurança utilizados e informar aos gestores os riscos residuais.

5.4.5 Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança.

5.4.6 Implantar controles que gerem registros auditáveis que permitam a rastreabilidade para fins de auditoria ou investigação.

5.4.7 Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o Prefeitura Municipal de Itapuí.

5.4.8 Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações.

5.4.9 Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança da informação.

5.4.10 Planejar, implantar e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

5.4.11 Atribuir a cada servidor/colaborar conta de acesso (individual) a computadores, dispositivo, sistemas, bases de dados ou a qualquer outro ativo de informação que se fizer necessário para realização de suas atividades, tornando possível identificá-lo como responsável por suas ações.

5.4.12 Realizar análise para mitigação do risco.

5.4.13 Criar perfis de acesso a fim de restringir ao mínimo necessário os poderes de cada indivíduo.

5.4.14 Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

5.4.15 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.

5.4.16 Definir as regras para instalação de software e hardware em ambiente de produção corporativo.

5.4.17 Monitorar o ambiente de TI registrando incidentes de segurança (vírus, trojans, furtos, acessos indevidos e assim por diante).

5.4.18 Garantir que todos os servidores e estações de trabalho tenham instalados políticas de segurança e antivírus corporativo atualizados.

5.4.19 Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos de informação da PMI.



# 6. POLÍTICAS

## 6.1 Controle de Acesso Lógico

6.1.1 A conta de acesso é o instrumento para identificação do usuário na rede da PMI sendo individual e o seu compartilhamento não permitido. O responsável

pela conta de acesso responde por toda e qualquer ação realizada mediante utilização de sua conta de acesso.

6.1.2 A concessão de privilégios de acesso deve ser realizada em conformidade com o princípio do privilégio mínimo, ou seja, cada credencial de acesso deve possuir apenas o conjunto de privilégios estritamente necessários ao desempenho das suas atribuições profissionais.

6.1.3 A concessão de acesso remoto a ativos de tecnologia da informação, deve ser precedida de autorização do custodiante do ativo, após análise da justificativa fornecida pelo gestor explicitando a necessidade do acesso. Este acesso deve contemplar somente os ativos necessários à realização do serviço, utilizar canal seguro e ser concedido em caráter provisório.

6.1.4 Cabe ao gestor responsável por pessoas ou processos, solicitar por ofício ou e-mail corporativo ao setor de TI, a concessão de permissão de acesso ao sistema em questão, bem como informar alterações de atribuições dos colaboradores imediatamente para adequação dos privilégios de acesso.

6.1.5 Todas as senhas de usuários comuns para autenticação na rede da PMI devem seguir os seguintes critérios mínimos:

6.1.6 A senha deve ser constituída de, no mínimo, 6 (seis) caracteres, sendo obrigatório o uso de caracteres alfanuméricos (letras e números), especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível;

6.1.7 A senha não deve ser baseada em informações pessoais, como próprio nome, data de nascimento, entre outros.

6.1.8 A data de expiração da senha deve ser de no máximo 90 dias, caso não seja alterada, esta será bloqueada;

6.1.9 Será obrigatória a troca de senha ao efetuar o primeiro login;

6.1.10 A base de dados de senhas deve ser armazenada com criptografia;

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

6.1.12 Qualquer anormalidade percebida pelo usuário quanto ao privilégio de seu acesso aos recursos de tecnologia da informação deve ser imediatamente comunicada a equipe de Tecnologia da Informação;

6.1.13 As contas com privilégio de administração de rede devem ser utilizadas somente para execução das atividades correspondentes à administração do ambiente conforme as responsabilidades atribuídas. As variáveis necessárias para acesso e administração devem ser de conhecimento restrito aos administradores dos equipamentos de rede.

## 6.2 Controle de Acesso à Infraestrutura

6.2.1 O acesso ao datacenter é restrito aos funcionários do setor de TI, o acesso por terceiros, como prestadores de serviço, deverá sempre ser acompanhado de um funcionário do setor. O mesmo se aplica a funcionários de outros setores .

6.2.2 O datacenter deverá monitorado por câmera de segurança.

6.2.3 A porta de acesso ao datacenter deve permanecer fechada, mesmo quando houver funcionários autorizados em suas dependências.

6.2.4 Bloqueio de acesso a funcionários desligados, o setor de Recursos Humanos deverá informar ao setor de suporte ou à divisão de tecnologia da informação, quando houver este desligamento para que as credenciais de acesso aos sistemas, computadores, e-mail e ambiente de rede, sejam bloqueadas.



## 6.3 Controle de Acesso à Internet

6.3.1 Como condição de uso, as áreas, serviços e conteúdo da empresa não poderão ser usados para quaisquer propósitos que sejam ilegais ou proibidos por esta Política de Uso, de modo a danificar, desativar, sobrecarregar ou prejudicar qualquer área, serviço ou conteúdo, ou interferir no uso e participação de qualquer um dos colaboradores. Não é permitido tentar obter acesso não-autorizado a qualquer área, serviço ou conteúdo dos sistemas ou redes de

computadores conectados, através de ações mal-intencionadas, corrupção de senha ou outros meios.

6.3.2 O uso e o acesso pelo colaborador à rede corporativa, computadores, Internet e/ou utilização de e-mail corporativo, deverão ser exclusivos para uso profissional, para a execução e desempenho dos objetivos da empresa. Exceto, nestes casos, deverá existir autorização expressa do superior hierárquico.

6.3.3 A PMI reafirma que o uso da Internet é uma ferramenta valiosa para seus negócios. Entretanto, o mau uso desta facilidade pode ter impacto negativo sobre a produtividade dos colaboradores e a própria reputação da mesma.

6.3.4 Todos os recursos tecnológicos da PMI existem para o propósito exclusivo de para a realização de tarefas relacionadas a gestão pública.

6.3.5 A PMI possui softwares e sistemas implantados que podem monitorar o uso da Internet, e-mails, chats, etc., através da rede local e das estações de trabalho da empresa.

6.3.6 A PMI se reserva o direito de inspecionar, sem a necessidade de aviso prévio, as estações de trabalho e qualquer arquivo armazenado, estejam no disco local da estação ou nas áreas privadas da rede, assim como monitorar o volume de tráfego na Internet e na Rede juntamente com os endereços web (http://) visitados, visando assegurar o cumprimento desta política.

6.3.7 O acesso à Internet para propósitos particulares ou estranhos às atividades da empresa poderá ser bloqueado, sem prévia comunicação ao colaborador, sem prejuízo das demais sanções aplicáveis.

6.3.8 Não é permitida a navegação aos sites pertencentes às categorias abaixo, e tampouco a exposição, o armazenamento, a distribuição, a edição, a gravação através do uso dos recursos computacionais e de comunicação da empregadora:

a) Material sexualmente explícito (em especial pedofilia) e ainda material contrário à moral ou aos bons costumes;

b) Material de conteúdo impróprio, ofensivo, preconceituoso ou discriminatório;

c) Apologia à violência ou ao terrorismo;

d) Apologia às drogas;

e) Violação de direito autoral (pirataria);

f) Execução de quaisquer tipos ou formas de fraudes;

g) Compartilhamento de arquivos estranhos às atividades da empresa e não autorizados pelo superior hierárquico.

6.3.9 Não é permitida a troca de arquivos de vídeo ou música.

6.3.10 É proibida a transferência de qualquer tipo de programa, jogo e similares para a rede interna da empresa sem autorização específica do superior hierárquico.

6.3.11 É proibido *downloads* de arquivos de extensões tipo: exe, .mp3, .wav, .bat, .com, .sys, .scr, .ppt, .mpeg, .avi, .rmvb, .dll, e de programas de entretenimento ou jogos, **exceto** os estritamente relacionados aos serviços inerentes à função do colaborador com vistas às atividades da PMI.

6.3.12 Não é permitido o acesso a programas de TV na Internet ou qualquer conteúdo sob demanda (*streaming* como Youtube, Netflix, Spotify, Deezer, Rádio Online).

6.3.13 É proibido o uso de jogos, inclusive os de Internet (*onlines*).

6.3.14 O uso do e-mail corporativo não garante direito sobre este, nem confere autoridade para liberar acesso à outras pessoas, pois se constitui de informações pertencentes à PMI.

6.3.15 O colaborador não poderá revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de suas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial;

6.3.16 O colaborador que divulgar informações confidenciais da **PMI** em grupos de discussão, bate-papos, Instant Messaging, e-mail, telefone, não importando se a divulgação foi deliberada ou inadvertida, poderá sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei, responsabilidade criminal ou civil.

6.3.17 Sendo de interesse da **PMI** que os seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços de notícias é aceitável, desde que o seu uso não comprometa o uso de Banda da rede, nem perturbe o bom andamento dos trabalhos, observados em todos os casos os termos desta política de uso.

6.3.18 A utilização da Internet para atividades não relacionadas com as rotinas da **PMI** é facultada durante o horário de almoço, desde que dentro das regras de uso definidas nesta política.

6.3.19 Cada colaborador com acesso à rede (arquivos compartilhados no servidor) e/ou sistemas (SIS, SIA7, SCPI8, SIP8, SIA 7.5, ESUS, SIMBOLUS) recebe um código de identificação (login) e uma senha (password), ambos são pessoais e confidenciais, não sendo permitido o seu empréstimo a quem quer que seja. Os colaboradores que se utilizarem de códigos de identificação e de senhas de terceiros poderão ser demitidos por justa causa, sem prejuízo de outras cominações pertinentes.

6.3.20 O uso de qualquer recurso da **PMI** para atividades ilegais poderá ser utilizado para (penalidades) por justa causa e a **PMI** cooperará ativamente com as autoridades policiais ou judiciais nesses casos.

6.3.21 É proibida a saída de qualquer equipamento de propriedade da **PMI** pelo colaborador, exceto se houver autorização por expresso neste sentido formalizada por documento escrito e assinado.

6.3.22 A entrada e consequente uso de equipamentos de informática pessoais tais como *smartphone, tablets* e *notebooks*, deverá ser comunicada à **PMI**, em especial se for de qualquer forma utilizada qualquer de suas redes, inclusive Internet. **Em hipótese alguma a PMI será responsabilizada por danos no equipamento pessoal do colaborador ou, ainda, em casos de furto ou roubo.**

6.3.23 O presente Termo ficará permanentemente à disposição inclusive na forma virtual para conhecimento de todos os colaboradores, sendo que não poderá ser alegado desconhecimento para eximir-se de quaisquer responsabilidades.

6.3.24 Caso o colaborador tenha alguma dúvida ou comentários sobre a Política de uso adotada pela **PMI**, deverá entrar em contato com o Responsável de seu departamento ou Setor de Tecnologia da Informação.

6.3.25 As excepcionalidades e os casos omissos deverão ser relatados para ao Responsável de seu departamento.

## 6.4 E-mail Corporativo

O objetivo desta norma é informar aos colaboradores da Prefeitura Municipal de Itapuí quais são as atividades permitidas e proibidas quanto ao uso do e-mail corporativo.

O e-mail corporativo da Prefeitura Municipal de Itapuí é para uso relacionado às atividades do servidor **exclusivamente** desempenho de sua função.

É, portanto, vedado aos servidores o uso do serviço de correio eletrônico corporativo com o objetivo de:

6.4.1 Utilização exclusiva do domínio e gerenciador contendo @itapui.sp.gov.br, portando, fica vedado a utilização de gerenciadores de e-mail ou qualquer outro tipo de domínio que não seja o nosso corporativo.

6.4.2 Praticar crimes e infrações de qualquer natureza;

6.4.3 Executar ações nocivas contra outros recursos computacionais da PMI ou de redes externas;

6.4.4 Distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório ou de qualquer forma contrária à lei e aos bons costumes;

6.4.5 Disseminar anúncios publicitários, mensagens de entretenimento e mensagens do tipo “corrente”, vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho de suas funções ou que possam ser considerados nocivos ao ambiente de rede da **PMI**;

6.4.6 Enviar arquivos de áudio, vídeo ou animações, salvo os que tenham relação com as funções institucionais desempenhadas pela **PMI**;

6.4.7 Enviar mensagens que incluam material protegido por direitos autorais sem a permissão do detentor dos direitos;

6.4.8 Divulgar, no todo ou em parte, os endereços eletrônicos corporativos constantes do catálogo de endereços do serviço;

6.4.9 Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o Prefeitura Municipal de Itapuí ou suas unidades vulneráveis a ações civis ou criminais;

6.4.10 Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

6.4.11 Executar outras atividades lesivas, tendentes a comprometer a intimidade de usuários, a segurança e a disponibilidade do sistema, ou a imagem institucional;

**É de responsabilidade do usuário do correio eletrônico:**

6.4.12 Manter em sigilo sua senha de acesso ao correio eletrônico;

6.4.13 Fechar o aplicativo de correio (cliente) toda vez que se ausentar, evitando o acesso indevido;

6.4.14 Comunicar imediatamente ao Setor de Tecnologia da Informação, recebimento de mensagens com vírus ou que venham a trazer algum tipo de dano aos sistemas de informática;

6.4.15 Efetuar a manutenção de sua caixa postal, evitando ultrapassar o limite de armazenamento e garantindo o seu funcionamento contínuo.

## 6.5 Uso de Equipamentos de Informática

O objetivo desta seção é estabelecer critérios na utilização dos equipamentos de informática na Prefeitura Municipal de Itapuí, sendo estas:

6.5.1 Os recursos computacionais somente devem ser utilizados para a execução de atividades de interesse da PMI;

6.5.2 Cada estação de trabalho possui controle de IP (Identificação de dispositivo), os quais permitem que ela seja identificada na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário;

6.5.3 Não é permitido gravar nas estações de trabalho e na Rede da PMI: mp3, filmes, fotos e software com direitos autorais ou qualquer outro tipo que possa ser considerado pirataria;

6.5.4 Todos os dados relativos às atividades da Secretaria devem ser mantidos no Servidor de Arquivos, onde existe sistema de backup diário e confiável, quando não disponível o recurso de Servidor de Arquivo, o próprio usuário deve fazer cópia de segurança dos arquivos locais e verificar o que pode ser eliminado, evitando acúmulo de dados desnecessários;

6.5.5. Os arquivos gravados em diretórios temporários (pastas públicas) podem ser acessados por todos os usuários que utilizarem a rede local, portanto não garante sua integridade, podendo ser alterados ou excluídos sem prévio aviso e por qualquer usuário;

6.5.6. Não será feito cópia de segurança dos arquivos criados no computador local dos colaboradores. O próprio usuário deve fazer cópia de segurança dos arquivos locais e verificar o que pode ser eliminado, evitando acúmulo de dados desnecessários;

6.5.7. É proibida a abertura de computadores para qualquer tipo de reparo, caso seja necessário o reparo deverá ocorrer pelo suporte técnico do setor de Tecnologia da Informação da PMI;

6.5.8. Quanto à utilização de equipamentos de informática particulares (celulares, notebooks, tablets e/ou qualquer dispositivos móveis que venham acessar a

rede sem fio ou rede estruturada) o colaborador deverá comunicar a chefia imediata, que solicitará sua liberação de acesso através da Gerência de Tecnologia da Informação;

6.5.9. Em caso de dano, inutilização ou extravio do equipamento o colaborador deverá comunicar imediatamente o setor de Tecnologia da Informação que deverá adotar as providências cabíveis;

6.5.10 Em caso de furto ou roubo, providenciar Boletim de Ocorrência junto à Polícia Civil e entregá-lo no setor de Tecnologia da Informação, que deverá adotar as providências cabíveis;

6.5.11 É proibida a colocação de adesivos com imãs nos equipamentos;

6.5.12 É dever do colaborador zelar pela integridade do equipamento estritamente como instrumento de trabalho, juntamente com os acessórios que foram utilizados;

6.5.13 É de inteira responsabilidade do colaborador, ao receber o Termo de Responsabilidade, verificar as informações nele contidas como Tombamento, série, além dos seus dados pessoais, matrícula e unidade de trabalho;

6.5.14 Não é permitido alterar as configurações de rede e da BIOS das máquinas, bem como, efetuar qualquer modificação que possa causar algum problema futuro;

6.5.15 Fica proibida a utilização, sem devido consentimento, da utilização de equipamentos de informática por pessoas sem vínculo com a Prefeitura Municipal de Itapuí;

6.5.16 É vedado retirar e/ou danificar placas identificadoras de patrimônio, travas e lacres de segurança dos equipamentos de informática;

6.5.17 Não é permitido conectar e/ou configurar equipamento à rede, sem a prévia liberação da Gerência de Tecnologia da Informação;

6.5.18 O antivírus ou respectivos módulos de segurança devem estar atualizados e com a autoproteção ativa na estação de trabalho;

6.5.19 Os equipamentos considerados críticos ao desempenho das atividades da PMI devem ser armazenados em áreas apropriadas, com acesso restrito e, sempre que possível, controlado por dispositivos de identificação;

6.5.20 O acesso de colaboradores/visitantes às áreas que hospedam equipamentos críticos deverá ser autorizado pelo custodiante e acompanhado de um servidor público. A restrição de acesso deve estar alinhada aos riscos identificados;

6.5.21 Os equiapmentos *notebook*s deveverão ser utilizado exclusivamente para o desenvolvimento das atividades profissionais do(a) servidor(a) público(a) junto ao Município de Itapuí;

6.5.22 O *notebook* não deverá ser usado fora das dependências da **PMI**;

6.5.23 Não poderão ser instalados softwares no *notebook* em questão sem a autorização do(a) servidor(a)público(a)responsável pelo setor municipal de Tecnologia da Informação;

6.5.24 Arquivos pessoais não poderão ser armazenados no *notebook*, podendo, inclusive, serem excluídos sem prévia consulta em eventual formatação a ser realizada pelo setor municipal de tecnologia da informação;

6.5.25 É de responsabilidade do(a) servidor(a) público(a) zelar pelo bom uso do *notebook*, evitando a quebra, a exposição ao sol e outros procedimentos que inibam o bom funcionamento do equipamento;

6.5.26 Em caso de furto ou roubo, o(a) servidor(a) público(a) deverá comunicar imediatamente o seu superior hierárquico, bem como o(a)servidor(a) público(a) responsável pelo setor municipal de Tecnologia da Informação;

6.5.27 Para reposição do *notebook* por mau uso ou perda, o valor de pagamento do equipamento será o mesmo que consta na nota fiscal de aquisição do bem, devidamente atualizado pelo índice INPC/IBGE.



## 6.6 Backups

6.6.1 Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de backup" - períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

6.6.2 Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

6.6.3 As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.

6.6.4 As unidades de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome e, de preferência, com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

6.6.5 O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

6.6.6 É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

6.6.7 Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

6.6.8 É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de backup nos termos do Procedimento de Controle de Mídias de Backup.



## 6.7 Auditoria, monitoramento e registro de logs de acesso

Para garantir as regras mencionadas nesta PSI, a Prefeitura Municipal de Itapuí poderá:

6.7.1 Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos 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;

6.7.2 Tornar pública as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior);

6.7.3 Realizar, a qualquer momento, inspeção física nas máquinas de sua propriedade;

6.7.4 Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;

6.7.5 Credenciais de acesso serão registrados em logs automáticos, todos os acessos dos usuários aos recursos da Instituição, incluindo acesso aos sistemas, criação, exclusão e alteração de arquivos, horário de login na máquina, utilização de impressora e outros sistemas.

## 6.8 Política de Uso de Impressoras

6.8.1 A quantidade de impressões será registrada em Log e, poderá ser auditada quanto ao usuário que imprimiu, quantidade de páginas, nome do arquivo impresso.

6.8.2 O uso das impressoras deve ser feito para os interesses da Instituição e utilizadas com consciência ecológica.

# 7. CUMPRIMENTO

A Prefeitura Municipal de Itapuí 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 Municipalidade. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela Instituição.

Diante do descumprimento desta política em geral, o usuário poderá, a qualquer tempo, ser auditado, através da equipe de TI e poderá receber em consequência a aplicação de ações disciplinares cabíveis que se fizerem necessárias.

# 8. CONSIDERAÇÕES FINAIS

A PSI da Prefeitura Municipal de Itapuí se aplica a todos os servidores e colaboradores que utilizam os recursos tecnológicos da PMI e abrange toda a infraestrutura de TI de todas as unidades municipais.

As políticas de segurança definidas nesta PSI devem ser publicadas e amplamente promovida visando garantir a integridade dos dados e informações, e o comprometimento dos servidores quanto ao uso correto dos recursos de TI disponibilizados pelo Município.

A PSI será revisada anualmente pela Coordenadoria Geral de Processamento de Dados e submetida à aprovação da Secretaria de Administração.

Cabe à Coordenadoria Geral de Processamento de Dados dar suporte as diligências relativas à segurança da informação providas por auditorias internas ou externas.

## TERMO DE CIÊNCIA E COMPROMISSO COM CLÁUSULA DE CONFIDENCIALIDADE

**Objetivo**

Definir as responsabilidades para todos os agentes públicos, estagiários e prestadores de serviços em atividade na Prefeitura Municipal de Itapuí que tenham acesso aos recursos de tecnologia da informação ou à rede de computadores da instituição.

Pelo presente termo, declaro ter conhecimento da **Política de Segurança da Informação** da Prefeitura Municipal de Itapuí, disponível para consulta no portal www.itapui.sp.gov.br no menu Tecnologia da Informação, e concordo em aceitar suas regras.

Com autorização superior, estou recebendo uma conta com privilégios adequados ao exercício das atividades que aqui executo, a qual deverá ser utilizada somente para tal fim.

**Declaro** estar ciente de que minhas ações serão monitoradas de acordo com a **Política de Segurança da Informação** e qualquer alteração feita sob minha identificação, advinda de minha autenticação e autorização, é de minha responsabilidade e me **comprometo a não os disponibilizar ou os divulgar a entidades (pessoas, sistemas ou órgãos) não autorizadas**

Estou ciente, ainda, de minha responsabilidade pelo dano que possa causar por descumprimento da **Política de Segurança da Informação** da Prefeitura Municipal de Itapuí ao realizar uma ação de iniciativa própria de tentativa de modificação da configuração, física ou lógica, dos recursos computacionais sem a permissão da área competente.

Eu, _____,

inscrito(a) no CPF nº _____, colaborador, **declaro** que li e estou ciente da **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO** da Prefeitura Municipal de Itapuí e me **comprometo** a seguir todos os seus termos, bem como a me atualizar a respeito de eventuais alterações.



_____

Local, data e assinatura.