**PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA**

# DECRETO Nº 7.454, DE 16 DE JANEIRO DE 2026

Dispõe sobre a Política de Segurança da Informação (PSI) nos órgãos e entidades da Administração Pública Municipal e dá outras providências.

ANTONIO TAKASHI SASADA (ANTIAN), Prefeito do Município da Estância Turística de Paraguaçu Paulista, Estado de São Paulo, usando de atribuições que são conferidas pela legislação vigente e autorizado pela Legislação vigente;

DECRETA:

Art. 1º Fica instituída a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Municipal, conforme anexo, que tem como pressupostos básicos:

I - Confidencialidade: Garantir que as informações não estejam acessíveis ou reveladas a pessoas físicas, sistemas, órgãos ou entidades não autorizadas ou credenciadas;

II - Integridade: Garantir que as informações contidas nos recursos tecnológicos não sejam alteradas indevidamente ou destruídas de maneira não autorizada, seja intencionalmente ou acidentalmente;

III - Disponibilidade: Garantir que as informações estejam acessíveis e em condições de serem utilizadas por usuários ou custodiantes autorizados.

Art. 2° Para efeitos da Política de Segurança da Informação, ficam estabelecidos os seguintes conceitos:

I - Auditoria: Verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;

II - Não-repúdio: Utilizado para garantir que os usuários não possam negar uma ação ou operação de sua autoria;

III - Plano de Continuidade de Negócios: Aplicação de estratégias capazes de realizar a continuidade durante a disrupção, prontidão para continuidade e retomada de recursos em momentos de crise, evitando falhas catastróficas em processos críticos da instituição;

IV - Recursos de Tecnologia da Informação e Comunicação ou simplesmente “Recursos de TIC”: Ativos de hardware, software, serviços de conexão e comunicação ou infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações;

V - Segurança da Informação: Preservação da confidencialidade, integridade, disponibilidade da informação. Visa proteger a informação contra ameaças para garantir a continuidade dos negócios, minimizar danos e maximizar o retorno sobre investimentos e novas oportunidades de transação.

Art. 3° São diretrizes básicas da Política de Segurança da Informação:

I - Definir os padrões de implementação efetiva da segurança da informação, garantindo a proteção de dados em meios físicos e digitais atenção as melhores práticas estabelecidas pelas normas ABNT NBR ISO/IEC 27001 (Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de

gestão da segurança da informação - Requisitos) e ABNT NBR ISO/IEC 27002 (Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação);

II - Orientar os colaboradores da Prefeitura Municipal da Estância Turística de Paraguaçu Paulista a adotarem comportamentos alinhados com as necessidades do negócio e os requisitos legais de proteção de dados pessoais;

III - Promover ações para a manutenção da segurança da informação, criando normas específicas para sistemas de informação e assegurando a eficácia dos controles e processos estabelecidos;

IV - Manter todos os mecanismos de proteção para assegurar a segurança da informação, visando a continuidade no órgão;

V - Considerar toda informação gerada por colaboradores, utilizando recursos da Prefeitura, como propriedade do órgão;

VI - Reavaliar periodicamente as ameaças e riscos para assegurar a proteção do órgão;

VII - Restringir o acesso às informações produzidas ou recebidas às atribuições necessárias para o desempenho das atividades dos usuários;

VIII - Alinhar os processos de aquisição ou contratação de bens e recursos de TIC com a PSI e seus documentos auxiliares, em conformidade com a legislação vigente;

IX - Utilizar os equipamentos de informática e comunicação, sistemas e informações exclusivamente para o cumprimento das atividades profissionais;

X - Revisar e ajustar a PSI periodicamente, sempre que ocorrerem eventos ou fatos relevantes;

XI - Evitar a circulação de informações e/ou mídias confidenciais e assegurar que relatórios não sejam deixados em locais de fácil acesso;

XII - Aderir ao conceito de "mesa limpa", garantindo que, ao concluir o trabalho, não haja relatórios e/ou mídias confidenciais sobre as mesas;

XIII - Executar os procedimentos de gestão de continuidade do negócio em conformidade com os requisitos de segurança da informação da Prefeitura.

Art. 4º Serão adotadas as seguintes regras:

I - Assegurar que todos os mecanismos de proteção à segurança da informação sejam mantidos e que toda informação gerada seja considerada propriedade do órgão;

II - Reavaliar periodicamente as ameaças e riscos, garantindo que o acesso às informações seja restrito conforme as necessidades do desempenho das atividades;

III - Alinhar os processos de aquisição ou contratação de bens e recursos de TIC com a Política de Segurança da Informação e utilizar equipamentos e sistemas exclusivamente para atividades profissionais;

IV - Revisar e ajustar a Política de Segurança da Informação conforme eventos relevantes, evitando a circulação indevida de informações confidenciais e assegurando a prática de "mesa limpa";

V - Executar procedimentos de Continuidade do Negócio em conformidade com os requisitos de segurança da informação e permitir que o acesso à rede seja exclusivo e intransferível, sendo o usuário responsável por suas atividades;

VI - Restringir o acesso a recursos de TIC a colaboradores autorizados e implementar controles de acesso físico para proteger dados e arquivos da Prefeitura;

VII - Limitar o uso da internet a fins profissionais e possibilitar que os equipamentos e serviços de acesso sejam propriedade do órgão, com medidas de bloqueio de conteúdo impróprio;

VIII - Responsabilizar os colaboradores por suas ações na internet e restringir o uso de proxies, VPNs, e conteúdo não relacionados ao trabalho;

IX - Proibir alterações físicas em equipamentos de informática e propiciar que qualquer dano ou extravio seja comunicado imediatamente ao setor responsável;

X - Limitar o uso do e-mail corporativo a finalidades institucionais e proteger o acesso com senhas

seguras, evitando a divulgação e o uso inadequado;

XI - Responsabilizar cada colaborador pelo backup e organização de seus arquivos, garantindo o armazenamento adequado no servidor;

XII - Classificar as informações conforme seu nível de confidencialidade, estabelecendo critérios claros para cada área do órgão.

Art. 5º Instituído o Comitê de Privacidade de Segurança da Informação e Privacidade (CSIP), caberão as seguintes atribuições:

I - Avaliar os mecanismos atuais de tratamento e proteção de dados pessoais no âmbito da Prefeitura, propondo políticas, estratégias e metas que assegurem a conformidade operacional da Controladora com as disposições da Lei n.º 13.709/2018 (Lei Geral de Proteção De Dados - LGPD);

II - Analisar assuntos relacionados à Segurança da Informação em atenção as melhores práticas estabelecidas pelas normas ABNT NBR ISO/IEC 27001 (Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos) e ABNT NBR ISO/IEC 27002 (Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação);

III - Propor princípios, diretrizes e regras para a gestão de dados pessoais;

IV - Propor políticas, procedimentos e planos para regulamentar a gestão de dados pessoais pelos agentes internos e externos que tratam dados pessoais em nome do controlador ou em função do cumprimento do contrato firmado com o controlador;

V - Prestar orientações sobre o tratamento e a proteção de dados pessoais de acordo com as diretrizes estabelecidas na LGPD e documentos internos sobre o tema;

VI - Promover a comunicação interna e externa acerca das medidas de proteção de dados adotadas, de ofício ou mediante provocação do interessado pessoais outros órgãos;

VII - Auxiliar o(a) Encarregado(a) de Dados na auditoria do tratamento realizado pelos operadores de dados pessoais;

VIII - Sugerir sanções administrativas quando houver violação às políticas pré-estabelecidas;

IX - Auxiliar nos trabalhos do(a) Encarregado(a) de Dados, garantindo-lhe a autonomia necessária ao exercício do seu encargo legal.

Parágrafo único. O funcionamento e as atribuições do Comitê de Segurança da Informação e Privacidade (CSIP) serão regulados em decreto específico.

Art. 6º Este decreto entra em vigor na data de sua publicação.

Paraguaçu Paulista, na data da assinatura digital.

**ANTONIO TAKASHI SASADA (ANTIAN)**

Prefeito

**EMERSON MARTINS DOS SANTOS**

Respondendo temporariamente pela Chefia de Gabinete do Prefeito

---

Documento assinado eletronicamente por **Emerson Martins dos Santos**, **Chefe de Gabinete do Prefeito**, em 19/01/2026, às 07:36, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

Documento assinado eletronicamente por **Antonio Takashi Sasada**, **Prefeito**, em 19/01/2026, às 11:15, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

A autenticidade deste documento pode ser conferida no site https://cidades.sei.sp.gov.br/marilia/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0131588** e o código CRC **D7DAAB1D**.

**Referência:** Processo nº 3535507.414.00007434/2025-11 SEI nº 0131588

**PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA**

MINUTA

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

**Processo SEI**: 3535507.414.00007434/2025-11

**Órgão Público**: PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA

**Tipo de Documento:** Política de Segurança da Informação

**Base Legal**: Decreto Municipal nº 7.454, de 16/01/2026.

## 1 OBJETIVO

O propósito deste documento é estabelecer diretrizes que orientem os colaboradores da **PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA,** inscrito no CNPJ sob o n.º 44.547.305/0001-93, doravante denominado apenas "**PREFEITURA**" a adotarem padrões de comportamento em conformidade com as necessidades de negócio e os requisitos legais de proteção de dados pessoais, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018 e Lei de Acesso à Informação (LAI) - Lei nº 12.527/2011.

Ademais, atribui-se a todas as áreas de negócios a responsabilidade de ajustar seus processos de acordo com os requisitos estabelecidos nesta política e pela Lei Geral de Proteção de Dados (LGPD).

Para os fins desta Política de Segurança da Informação ou simplesmente "PSI", a **PREFEITURA** adotará os seguintes princípios de Segurança da Informação para proteger as informações e os recursos tecnológicos sob sua propriedade ou guarda, tais como:

**a) Confidencialidade:** Garante que as informações não estejam acessíveis ou reveladas a pessoas físicas, sistemas, órgãos ou entidades não autorizadas ou credenciadas;

**b) Integridade**: Garante que as informações contidas nos recursos tecnológicos não sejam alteradas indevidamente ou destruídas de maneira não autorizada, seja intencionalmente ou acidentalmente;

**c) Disponibilidade:** Garante que as informações estejam acessíveis e em condições de serem utilizadas por usuários ou custodiantes autorizados.

## 2 VALIDADE

Esta PSI entrará em vigor na data da sua publicação, e terá vigência por prazo indeterminado, devendo-se revisá-la a cada período máximo de 16 (dezesseis) meses.

## 3 ABRANGÊNCIA

As diretrizes estabelecidas devem ser seguidas por todos os colaboradores que desempenham atividades na PREFEITURA, seja em órgãos da administração direta como em órgãos e entidades da administração indireta, bem como por qualquer pessoa ou empresa que tenha acesso a dados ou informações, em qualquer meio ou suporte.

Esta política informa a cada colaborador que os ambientes, sistemas, computadores e redes da instituição podem ser monitorados e gravados de acordo com as leis brasileiras.

Além disso, é responsabilidade de cada colaborador manter-se atualizado sobre esta PSI e sobre os procedimentos e normas relacionados, buscando orientação de seu gestor ou da Tecnologia da Informação

(TI) sempre que não estiver completamente seguro sobre a aquisição, uso, armazenamento ou descarte de informações.

**4 DEFINIÇÕES**

**a) Auditoria:** Verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;

**b) Classificação da informação:** Atribuição, pela autoridade competente, do grau de sigilo dado à informação, documento, material, área ou instalação;

**c) Controle de Acesso:** Conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

**d) Correio Eletrônico:** Método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;

**e) Dado:** Representação de uma informação, instrução ou conceito, de modo que possa ser armazenado e processado por um computador;

**f) Dispositivos Removíveis de Armazenamento de Informação**: Dispositivos que podem armazenar informações e serem removidos do equipamento, permitindo a portabilidade dos dados, como CDs, DVDs e pen drives;

**g) Estação de Trabalho:** Dispositivo utilizado por um colaborador para executar tarefas relacionadas às suas funções na **PREFEITURA**, incluindo desktops, laptops e terminais;

**h) Incidente de Segurança:** Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

**i ) *Peer-to-peer* (P2P):** Permite conectar o computador de um usuário a outro para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, entre outros;

**j) Recursos de Tecnologia da Informação e Comunicação ou simplesmente "Recursos de TIC":** Ativos de hardware, software, serviços de conexão e comunicação ou infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações;

**k) Segurança da Informação:** Preservação da confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação. Visa proteger a informação contra ameaças para garantir a continuidade dos negócios, minimizar danos e maximizar o retorno sobre investimentos e novas oportunidades de transação;

**l) Servidor de Rede:** Recurso de TIC com a finalidade de disponibilizar ou gerenciar serviços ou sistemas de informação;

**m) Usuário:** Servidores públicos municipais, cargos comissionados, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da **PREFEITURA**, solicitada via ofício e formalizada por meio da assinatura do Termo de Responsabilidade;

**n) VPN (*Virtual Private Network*):** Rede de dados privada que faz uso das infraestruturas públicas de telecomunicações, preservando a privacidade, sendo a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas. Com uma VPN, pode-se enviar dados entre dois computadores através de uma rede compartilhada ou pública de uma maneira que emula uma conexão ponto a ponto privada.

**5 DIRETRIZES**

São diretrizes de Segurança da Informação no âmbito da **PREFEITURA**:

**a)** Todos os mecanismos de proteção empregados para garantir a segurança da informação devem ser mantidos a fim de assegurar o princípio da continuidade na Instituição;

**b)** Qualquer informação gerada pelos colaboradores, utilizando total ou parcialmente recursos da **PREFEITURA**, é propriedade da instituição;

**c)** As ameaças e riscos devem ser periodicamente reavaliados para garantir a efetiva proteção da Instituição;

**d)** O acesso às informações produzidas ou recebidas pelas Secretarias/Departamentos Municipais deve ser restrito às atribuições necessárias para o desempenho das atividades correspondentes por parte dos usuários/colaboradores;

**e)** Os processos de aquisição ou contratação de bens e serviços de tecnologia da informação devem estar alinhados com esta PSI e seus documentos auxiliares, em conformidade com a legislação vigente;

**f)** Os equipamentos de informática e comunicação, sistemas e informações devem ser utilizados exclusivamente para o cumprimento das atividades profissionais;

**g)** Esta PSI pode ser revisada periodicamente e, se necessário, ajustada sempre que ocorrerem eventos ou fatos relevantes;

**h)** Os colaboradores devem evitar a circulação de informações e/ou mídias consideradas confidenciais e/ou restritas, bem como devem garantir que não haja relatórios deixados em impressoras ou mídias em locais de fácil acesso;

**i)** Devem aderir ao conceito de "mesa limpa", ou seja, ao concluir o trabalho, garantir que não haja nenhum relatório e/ou mídia confidencial e/ou restrita sobre suas mesas;

**j)** Os procedimentos de gestão de Continuidade do Negócio devem ser executados em conformidade com os requisitos de segurança da informação da Prefeitura.

## 6 REGRAS GERAIS

### 6.1 Controle de Acesso

#### 6.1.1 Conta de Acesso

**6.1.1.1** A conta de acesso na rede da **PREFEITURA** é exclusiva e intransferível, e sua divulgação é estritamente proibida.

**6.1.1.2** O usuário é integralmente responsável por todas as atividades realizadas com sua identificação e senha de acesso.

#### 6.1.2 Segurança da Senha

As senhas dos usuários comuns devem seguir critérios mínimos:

**a)** Mínimo de 8 (oito) caracteres, incluindo letras e números;

**b)** Não repetir as duas últimas senhas utilizadas;

**c)** Troca de senha no primeiro acesso.

#### 6.1.3 Acesso aos Serviços de TI

**6.1.3.1** O acesso aos serviços de TI é concedido apenas a colaboradores autorizados pelas Secretarias.

**6.1.3.2** Qualquer anormalidade no acesso deve ser reportada imediatamente a Tecnologia da Informação (TI).

#### 6.1.4 Controle de Acesso Físico

**6.1.4.1** Os controles de acesso físico visam restringir o acesso não autorizado a dados e arquivos relacionados às atividades da **PREFEITURA**.

**6.1.4.2** O acesso as áreas internas são permitidas somente a pessoas autorizadas.

### 6.2 Uso da Internet

#### 6.2.1 Restrição de Conteúdo

**6.2.1.1** O acesso à Internet deve limitar-se a fins profissionais, relacionados às atividades institucionais.

**6.2.1.2** Cada usuário é responsável pelas ações e acessos realizados através de sua conta de acesso.

#### 6.2.2 Propriedade e Controle de Acesso

**6.2.2.1** Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são propriedade da instituição.

**6.2.2.2** A instituição reserva-se o direito de analisar e, se necessário, bloquear arquivos, sites, correios

eletrônicos, domínios ou aplicativos na rede/internet, a fim de garantir o cumprimento desta Política de Segurança da Informação;

**6.2.3 Restrições de Acesso**

**6.2.3.1** É proibido acessar conteúdos ofensivos, ilegais ou impróprios, incluindo pornografia, pedofilia, preconceitos, vandalismo, entre outros.

**6.2.3.2** Não é permitido o uso recreativo da internet durante o horário de expediente.

**6.2.3.3** O uso de proxies anônimos, VPNs, e tuteladores, assim como o acesso a rádio, TV em tempo real, jogos, e outros conteúdos não relacionados ao trabalho são estritamente proibidos.

**6.2.4 Bloqueios**

A instituição poderá bloquear o acesso a arquivos e sites não autorizados que comprometam o desempenho da rede ou a produtividade do colaborador, além de expor a rede a riscos de segurança.

**6.2.5 Consequências da Utilização Irregular**

**6.2.5.1** Em caso de utilização irregular, o usuário poderá ter seu acesso à Internet bloqueado, sendo comunicado à sua chefia imediata.

**6.2.5.2** O envolvimento em práticas irregulares pode resultar em processo administrativo disciplinar e nas sanções legais aplicáveis, garantindo-se o direito ao contraditório e à ampla defesa.

**6.3 Uso de Recursos de Computacionais**

**6.3.1** Os recursos computacionais devem ser exclusivamente utilizados para a execução de atividades relacionadas aos interesses da **PREFEITURA**.

**6.3.2** Cada estação de trabalho possui um controle de IP (Protocolo Internet) que a identifica na rede. Portanto, todas as atividades realizadas na estação de trabalho são de responsabilidade do usuário. É fundamental que o usuário faça o *logoff* ou bloqueie a estação de trabalho ao se ausentar do ambiente de trabalho.

**6.3.3** Arquivos armazenados em diretórios temporários (pastas públicas) podem ser acessados por todos os usuários da rede local, o que não garante sua integridade e pode resultar em alterações ou exclusões não autorizadas.

**6.3.4** É proibida a abertura física dos computadores para qualquer finalidade. Caso seja necessário realizar reparos, estes devem ser encaminhados ao setor de Tecnologia da Informação.

**6.3.5** Em caso de dano, inutilização ou extravio de equipamentos, o colaborador deve comunicar imediatamente ao setor de patrimônio, que tomará as providências necessárias.

**6.3.6** É proibido realizar alterações físicas nos equipamentos de informática.

**6.3.7** O colaborador deve zelar pela integridade do equipamento e de seus acessórios, tratando-os estritamente como instrumentos de trabalho.

**6.3.8** Não é permitido alterar as configurações de rede e da BIOS (*Basic Input/Output System*) das máquinas, nem fazer modificações que possam resultar em problemas futuros.

**6.3.9** Não é permitido retirar ou transportar equipamentos de informática da **PREFEITURA** sem autorização prévia do secretário da pasta.

**6.3.10** É proibido o uso não autorizado de equipamentos de informática por pessoas sem vínculo com a **PREFEITURA**.

**6.3.11** É vedado retirar ou danificar placas identificadoras de patrimônio, travas e lacres de segurança dos equipamentos de informática.

**6.4 Uso de E-mail Corporativo**

**6.4.1** O colaborador, a critério de seu chefe imediato e de acordo com as necessidades de serviço e recomendações, poderá ter acesso a uma conta de e-mail oficial, sendo solicitado ao departamento de Tecnologia da Informação (TI).

**6.4.2** O acesso ao serviço de e-mail é protegido por uma senha pessoal e intransferível, sendo proibida sua

divulgação.

**6.4.3** É proibido ao usuário utilizar o serviço de e-mail corporativo com as seguintes finalidades:

**a)** Praticar crimes e infrações de qualquer natureza;

**b)** Realizar ações prejudiciais contra os recursos computacionais da **PREFEITURA** ou de redes externas;

**c)** Distribuir conteúdo obsceno, pornográfico, ofensivo, preconceituoso, discriminatório ou ilegal;

**d)** Enviar anúncios publicitários, mensagens de entretenimento, mensagens de corrente, vírus ou qualquer outro programa de computador que não esteja relacionado com as funções institucionais;

**e)** Compartilhar arquivos de áudio, vídeo ou animações, exceto aqueles relacionados com as atividades institucionais da **PREFEITURA**;

**f)** Realizar outras atividades prejudiciais que possam comprometer a privacidade dos usuários, a segurança do sistema ou a imagem da instituição.

**6.4.4 É responsabilidade do usuário do e-mail corporativo:**

**a)** Manter a senha de acesso ao e-mail em sigilo;

**b)** Fechar o sistema de e-mail (navegador/*browser*) ao se ausentar para evitar acessos não autorizados;

**c)** Gerenciar regularmente a caixa de entrada do e-mail, evitando exceder o limite de armazenamento e garantindo o funcionamento contínuo.

**6.5 *Backups***

**6.5.1** Não será realizado *backup* dos arquivos criados nas estações de trabalho dos colaboradores. Cada usuário é responsável por fazer *backup* de seus arquivos locais e por gerenciar o armazenamento, evitando acumulação desnecessária de dados.

**6.5.2** Cada usuário é responsável pelo armazenamento dos arquivos relacionados à sua unidade no servidor, garantindo assim a realização do *backup* deles.

**6.5.3** É responsabilidade do usuário manter organizado o diretório ao qual tem acesso, evitando o acúmulo de arquivos duplicados e desordenados.

**6.6 Classificação da Informação**

**6.6.1** É responsabilidade do responsável de cada pasta estabelecer critérios relacionados ao nível de confidencialidade das informações (relatórios e/ou mídias) geradas por sua área, conforme a seguinte tabela:

**a) Pública:** Engloba informações acessíveis a usuários da instituição, clientes, fornecedores, prestadores de serviços e público em geral;

**b) Interna:** Abrange informações acessíveis somente aos funcionários da instituição, caracterizadas por um grau de confidencialidade que pode afetar a imagem da organização;

**c) Confidencial:** Compreende informações acessíveis aos usuários da instituição e aos parceiros da organização. A divulgação não autorizada dessas informações pode causar impacto financeiro, de imagem ou operacional no negócio da organização ou do parceiro;

**d) Restrita:** Refere-se a informações acessíveis apenas aos usuários da instituição explicitamente indicados pelo nome ou pela área a que pertencem. A divulgação não autorizada dessas informações pode ocasionar danos significativos ao negócio e/ou comprometer a estratégia empresarial da organização.

**7 PAPÉIS E RESPONSABILIDADES**

**7.1 Alta Direção:**

**a)** Assegurar o cumprimento desta PSI e demais documentos correlatos por parte de seus colaboradores e prestadores de serviços.

**7.2 Tecnologia da Informação (TI):**

**a)** Promover e incentivar a conscientização sobre segurança da informação e comunicações entre os colaboradores;

**b)** Acompanhar investigações e avaliações de danos resultantes de violações de segurança;

**c)** Propor recursos necessários para a implementação das medidas de segurança da informação e comunicações;

**d)** Realizar estudos sobre novas tecnologias e avaliar seus possíveis impactos na segurança da informação e comunicações;

**e)** Receber, organizar, armazenar e tratar adequadamente informações sobre eventos e incidentes de segurança, informando os gestores pertinentes sobre ações corretivas ou de contingência em cada caso.

**7.2 Secretários e Gestores:**

**a)** Cumprir, fazer cumprir e gerenciar o cumprimento desta PSI, naquilo que for aplicável por parte de seus colaboradores.

**7.3 Recursos Humanos:**

**a)** Divulgar e garantir a ciência dos novos colaboradores ao Estatuto do Servidor [inserir] e Políticas de Segurança e Privacidade, da **PREFEITURA** no momento da contratação.

**7.4 Colaboradores:**

**a)** Proteger ativamente as informações confidenciais da organização, mantendo a confidencialidade, integridade e disponibilidade dos dados a que tenha acesso;

**b)** Seguir rigorosamente as Políticas de Segurança da Informação e Privacidade estabelecidas pela **PREFEITURA**;

**c)** Reportar imediatamente ao Secretário da respectiva pasta quaisquer incidentes de Segurança da Informação, suspeitas de violação ou comportamentos inadequados;

**d)** Participar dos treinamentos e atividades de conscientização em Segurança da Informação e Privacidade para manter-se atualizado sobre as melhores práticas e ameaças emergentes;

**e)** Utilizar apenas os recursos de tecnologia da informação autorizados e não alterar quaisquer medidas de segurança em suas atividades cotidianas.

## 8 PENALIDADES

Qualquer violação as disposições estabelecidas nesta PSI incorrerão na aplicação das penalidades cabíveis previstas no Estatuto do Servidor [inserir] da **PREFEITURA**, cláusulas contratuais e legislação aplicável vigente.

## 9 CONTROLE DE VERSIONAMENTO

| SIGLA | VERSÃO | VIGÊNCIA | RESPONSÁVEL | CONTROLE DAS MODIFICAÇÕES |
|---|---|---|---|---|
| **PSI** | 1.0 | [Inserir data publicação do decreto] | [Inserir responsável pela aprovação] | Primeira versão. |

## 10 DISPOSIÇÕES FINAIS

**10.1** O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as Normas, Políticas e Procedimentos aplicáveis pela **PREFEITURA**.

**10.2** Os casos omissos serão remetidos ao Comitê de Segurança da Informação e Privacidade (CSIP) para avaliação.

**10.3** Qualquer dúvida relativa a esta PSI deve ser encaminhada para o endereço eletrônico [inserir].

**10.4** Esta Política entra em vigor na data de sua instituição por decreto.

## 11 ANEXOS

**ANEXO I –** Termo de Ciência da Política de Segurança da Informação (Pessoa Física - PF)

**ANEXO II –** Termo de Ciência da Política de Segurança da Informação (Pessoa Jurídica - PJ)

Paraguaçu Paulista, na data da assinatura digital.

**ANTONIO TAKASHI SASADA (ANTIAN)**
Prefeito

**EMERSON MARTINS DOS SANTOS**
Respondendo temporariamente pela Chefia de Gabinete do Prefeito

Documento assinado eletronicamente por **Emerson Martins dos Santos**, **Chefe de Gabinete do Prefeito**, em 19/01/2026, às 07:36, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

Documento assinado eletronicamente por **Antonio Takashi Sasada**, **Prefeito**, em 19/01/2026, às 11:15, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

A autenticidade deste documento pode ser conferida no site https://cidades.sei.sp.gov.br/marilia/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0131591** e o código CRC **0645F9B4**.

**Referência:** Processo nº 3535507.414.00007434/2025-11 SEI nº 0131591

**PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA**

MINUTA

# TERMO DE CIÊNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PESSOA FÍSICA - PF)

**Processo SEI**: 3535507.414.00007434/2025-11

**Órgão Público**: PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA

**Tipo de Documento:** Termo de Ciência (Pessoa Física - PF)

**Base Legal**: Decreto Municipal nº 7.454, de 16/01/2026.

Pelo presente instrumento, **[NOME COMPLETO]**, inscrito(a) no CPF sob o nº XXX.XXX.XXX-XX, DECLARA para os devidos fins que tomou conhecimento e compreendeu as disposições previstas na Política de Segurança da Informação, instituída pela **PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA,** inscrita no CNPJ n.º 44.547.305/0001-93, se comprometendo a respeitar, no desempenho de suas obrigações contratualmente constituídas, todos os seus termos, condições e princípios, estando sujeito(a) às responsabilidades cabíveis advindas do descumprimento.

Paraguaçu Paulista, na data da assinatura digital.

**[NOME DO SIGNATÁRIO]**

[Cargo do Signatário]

Documento assinado eletronicamente por **Antonio Takashi Sasada**, **Prefeito**, em 19/01/2026, às 11:15, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

Documento assinado eletronicamente por **Emerson Martins dos Santos**, **Chefe de Gabinete do Prefeito**, em 19/01/2026, às 12:28, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

A autenticidade deste documento pode ser conferida no site https://cidades.sei.sp.gov.br/marilia/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0131594** e o código CRC **5828B197**.

**PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA**

MINUTA

# TERMO DE CIÊNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PESSOA JURÍDICA - PJ)

**Processo SEI**: 3535507.414.00007434/2025-11

**Órgão Público**: PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA

**Tipo de Documento:** Termo de Ciência (Pessoa Jurídica - PJ)

**Base Legal**: Decreto Municipal nº 7.454, de 16/01/2026.

Pelo presente instrumento, a(o) **[RAZÃO SOCIAL]**, inscrito(a) no CNPJ sob o nº XXX.XXX.XXX-XX, DECLARA para os devidos fins que tomou conhecimento e compreendeu as disposições previstas na Política de Segurança da Informação instituída pela **PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA**, inscrita no CNPJ n.º 44.547.305/0001-93, se comprometendo a respeitar, no desempenho de suas obrigações contratualmente constituídas, todos os seus termos, condições e princípios, estando sujeito(a) às responsabilidades cabíveis advindas do descumprimento.

Paraguaçu Paulista, na data da assinatura digital.

**[NOME DO SIGNATÁRIO]**

[Cargo do Signatário]

Documento assinado eletronicamente por **Antonio Takashi Sasada**, **Prefeito**, em 19/01/2026, às 11:15, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

Documento assinado eletronicamente por **Emerson Martins dos Santos**, **Chefe de Gabinete do Prefeito**, em 19/01/2026, às 12:27, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

A autenticidade deste documento pode ser conferida no site https://cidades.sei.sp.gov.br/marilia/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0131595** e o código CRC **A61F9D77**.

**PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA**

# DECRETO Nº 7.454, DE 16 DE JANEIRO DE 2026

Dispõe sobre a Política de Segurança da Informação (PSI) nos órgãos e entidades da Administração Pública Municipal e dá outras providências.

ANTONIO TAKASHI SASADA (ANTIAN), Prefeito do Município da Estância Turística de Paraguaçu Paulista, Estado de São Paulo, usando de atribuições que são conferidas pela legislação vigente e autorizado pela Legislação vigente;

DECRETA:

Art. 1º Fica instituída a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Municipal, conforme anexo, que tem como pressupostos básicos:

I - Confidencialidade: Garantir que as informações não estejam acessíveis ou reveladas a pessoas físicas, sistemas, órgãos ou entidades não autorizadas ou credenciadas;

II - Integridade: Garantir que as informações contidas nos recursos tecnológicos não sejam alteradas indevidamente ou destruídas de maneira não autorizada, seja intencionalmente ou acidentalmente;

III - Disponibilidade: Garantir que as informações estejam acessíveis e em condições de serem utilizadas por usuários ou custodiantes autorizados.

Art. 2° Para efeitos da Política de Segurança da Informação, ficam estabelecidos os seguintes conceitos:

I - Auditoria: Verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;

II - Não-repúdio: Utilizado para garantir que os usuários não possam negar uma ação ou operação de sua autoria;

III - Plano de Continuidade de Negócios: Aplicação de estratégias capazes de realizar a continuidade durante a disrupção, prontidão para continuidade e retomada de recursos em momentos de crise, evitando falhas catastróficas em processos críticos da instituição;

IV - Recursos de Tecnologia da Informação e Comunicação ou simplesmente “Recursos de TIC”: Ativos de hardware, software, serviços de conexão e comunicação ou infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações;

V - Segurança da Informação: Preservação da confidencialidade, integridade, disponibilidade da informação. Visa proteger a informação contra ameaças para garantir a continuidade dos negócios, minimizar danos e maximizar o retorno sobre investimentos e novas oportunidades de transação.

Art. 3° São diretrizes básicas da Política de Segurança da Informação:

I - Definir os padrões de implementação efetiva da segurança da informação, garantindo a proteção de dados em meios físicos e digitais atenção as melhores práticas estabelecidas pelas normas ABNT NBR ISO/IEC 27001 (Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de

gestão da segurança da informação - Requisitos) e ABNT NBR ISO/IEC 27002 (Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação);

II - Orientar os colaboradores da Prefeitura Municipal da Estância Turística de Paraguaçu Paulista a adotarem comportamentos alinhados com as necessidades do negócio e os requisitos legais de proteção de dados pessoais;

III - Promover ações para a manutenção da segurança da informação, criando normas específicas para sistemas de informação e assegurando a eficácia dos controles e processos estabelecidos;

IV - Manter todos os mecanismos de proteção para assegurar a segurança da informação, visando a continuidade no órgão;

V - Considerar toda informação gerada por colaboradores, utilizando recursos da Prefeitura, como propriedade do órgão;

VI - Reavaliar periodicamente as ameaças e riscos para assegurar a proteção do órgão;

VII - Restringir o acesso às informações produzidas ou recebidas às atribuições necessárias para o desempenho das atividades dos usuários;

VIII - Alinhar os processos de aquisição ou contratação de bens e recursos de TIC com a PSI e seus documentos auxiliares, em conformidade com a legislação vigente;

IX - Utilizar os equipamentos de informática e comunicação, sistemas e informações exclusivamente para o cumprimento das atividades profissionais;

X - Revisar e ajustar a PSI periodicamente, sempre que ocorrerem eventos ou fatos relevantes;

XI - Evitar a circulação de informações e/ou mídias confidenciais e assegurar que relatórios não sejam deixados em locais de fácil acesso;

XII - Aderir ao conceito de "mesa limpa", garantindo que, ao concluir o trabalho, não haja relatórios e/ou mídias confidenciais sobre as mesas;

XIII - Executar os procedimentos de gestão de continuidade do negócio em conformidade com os requisitos de segurança da informação da Prefeitura.

Art. 4º Serão adotadas as seguintes regras:

I - Assegurar que todos os mecanismos de proteção à segurança da informação sejam mantidos e que toda informação gerada seja considerada propriedade do órgão;

II - Reavaliar periodicamente as ameaças e riscos, garantindo que o acesso às informações seja restrito conforme as necessidades do desempenho das atividades;

III - Alinhar os processos de aquisição ou contratação de bens e recursos de TIC com a Política de Segurança da Informação e utilizar equipamentos e sistemas exclusivamente para atividades profissionais;

IV - Revisar e ajustar a Política de Segurança da Informação conforme eventos relevantes, evitando a circulação indevida de informações confidenciais e assegurando a prática de "mesa limpa";

V - Executar procedimentos de Continuidade do Negócio em conformidade com os requisitos de segurança da informação e permitir que o acesso à rede seja exclusivo e intransferível, sendo o usuário responsável por suas atividades;

VI - Restringir o acesso a recursos de TIC a colaboradores autorizados e implementar controles de acesso físico para proteger dados e arquivos da Prefeitura;

VII - Limitar o uso da internet a fins profissionais e possibilitar que os equipamentos e serviços de acesso sejam propriedade do órgão, com medidas de bloqueio de conteúdo impróprio;

VIII - Responsabilizar os colaboradores por suas ações na internet e restringir o uso de proxies, VPNs, e conteúdo não relacionados ao trabalho;

IX - Proibir alterações físicas em equipamentos de informática e propiciar que qualquer dano ou extravio seja comunicado imediatamente ao setor responsável;

X - Limitar o uso do e-mail corporativo a finalidades institucionais e proteger o acesso com senhas

seguras, evitando a divulgação e o uso inadequado;

XI - Responsabilizar cada colaborador pelo backup e organização de seus arquivos, garantindo o armazenamento adequado no servidor;

XII - Classificar as informações conforme seu nível de confidencialidade, estabelecendo critérios claros para cada área do órgão.

Art. 5º Instituído o Comitê de Privacidade de Segurança da Informação e Privacidade (CSIP), caberão as seguintes atribuições:

I - Avaliar os mecanismos atuais de tratamento e proteção de dados pessoais no âmbito da Prefeitura, propondo políticas, estratégias e metas que assegurem a conformidade operacional da Controladora com as disposições da Lei n.º 13.709/2018 (Lei Geral de Proteção De Dados - LGPD);

II - Analisar assuntos relacionados à Segurança da Informação em atenção as melhores práticas estabelecidas pelas normas ABNT NBR ISO/IEC 27001 (Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos) e ABNT NBR ISO/IEC 27002 (Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação);

III - Propor princípios, diretrizes e regras para a gestão de dados pessoais;

IV - Propor políticas, procedimentos e planos para regulamentar a gestão de dados pessoais pelos agentes internos e externos que tratam dados pessoais em nome do controlador ou em função do cumprimento do contrato firmado com o controlador;

V - Prestar orientações sobre o tratamento e a proteção de dados pessoais de acordo com as diretrizes estabelecidas na LGPD e documentos internos sobre o tema;

VI - Promover a comunicação interna e externa acerca das medidas de proteção de dados adotadas, de ofício ou mediante provocação do interessado pessoais outros órgãos;

VII - Auxiliar o(a) Encarregado(a) de Dados na auditoria do tratamento realizado pelos operadores de dados pessoais;

VIII - Sugerir sanções administrativas quando houver violação às políticas pré-estabelecidas;

IX - Auxiliar nos trabalhos do(a) Encarregado(a) de Dados, garantindo-lhe a autonomia necessária ao exercício do seu encargo legal.

Parágrafo único. O funcionamento e as atribuições do Comitê de Segurança da Informação e Privacidade (CSIP) serão regulados em decreto específico.

Art. 6º Este decreto entra em vigor na data de sua publicação.

Paraguaçu Paulista, na data da assinatura digital.

**ANTONIO TAKASHI SASADA (ANTIAN)**

Prefeito

**EMERSON MARTINS DOS SANTOS**

Respondendo temporariamente pela Chefia de Gabinete do Prefeito

Documento assinado eletronicamente por **Emerson Martins dos Santos**, **Chefe de Gabinete do Prefeito**, em 19/01/2026, às 07:36, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

Documento assinado eletronicamente por **Antonio Takashi Sasada**, **Prefeito**, em 19/01/2026, às 11:15, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

A autenticidade deste documento pode ser conferida no site https://cidades.sei.sp.gov.br/marilia/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0131588** e o código CRC **D7DAAB1D**.

**Referência:** Processo nº 3535507.414.00007434/2025-11 SEI nº 0131588

**PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA**

MINUTA

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

**Processo SEI**: 3535507.414.00007434/2025-11

**Órgão Público**: PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA

**Tipo de Documento:** Política de Segurança da Informação

**Base Legal**: Decreto Municipal nº 7.454, de 16/01/2026.

## 1 OBJETIVO

O propósito deste documento é estabelecer diretrizes que orientem os colaboradores da **PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA,** inscrito no CNPJ sob o n.º 44.547.305/0001-93, doravante denominado apenas "**PREFEITURA**" a adotarem padrões de comportamento em conformidade com as necessidades de negócio e os requisitos legais de proteção de dados pessoais, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018 e Lei de Acesso à Informação (LAI) - Lei nº 12.527/2011.

Ademais, atribui-se a todas as áreas de negócios a responsabilidade de ajustar seus processos de acordo com os requisitos estabelecidos nesta política e pela Lei Geral de Proteção de Dados (LGPD).

Para os fins desta Política de Segurança da Informação ou simplesmente "PSI", a **PREFEITURA** adotará os seguintes princípios de Segurança da Informação para proteger as informações e os recursos tecnológicos sob sua propriedade ou guarda, tais como:

**a) Confidencialidade:** Garante que as informações não estejam acessíveis ou reveladas a pessoas físicas, sistemas, órgãos ou entidades não autorizadas ou credenciadas;

**b) Integridade**: Garante que as informações contidas nos recursos tecnológicos não sejam alteradas indevidamente ou destruídas de maneira não autorizada, seja intencionalmente ou acidentalmente;

**c) Disponibilidade:** Garante que as informações estejam acessíveis e em condições de serem utilizadas por usuários ou custodiantes autorizados.

## 2 VALIDADE

Esta PSI entrará em vigor na data da sua publicação, e terá vigência por prazo indeterminado, devendo-se revisá-la a cada período máximo de 16 (dezesseis) meses.

## 3 ABRANGÊNCIA

As diretrizes estabelecidas devem ser seguidas por todos os colaboradores que desempenham atividades na PREFEITURA, seja em órgãos da administração direta como em órgãos e entidades da administração indireta, bem como por qualquer pessoa ou empresa que tenha acesso a dados ou informações, em qualquer meio ou suporte.

Esta política informa a cada colaborador que os ambientes, sistemas, computadores e redes da instituição podem ser monitorados e gravados de acordo com as leis brasileiras.

Além disso, é responsabilidade de cada colaborador manter-se atualizado sobre esta PSI e sobre os procedimentos e normas relacionados, buscando orientação de seu gestor ou da Tecnologia da Informação

(TI) sempre que não estiver completamente seguro sobre a aquisição, uso, armazenamento ou descarte de informações.

**4 DEFINIÇÕES**

**a) Auditoria:** Verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;

**b) Classificação da informação:** Atribuição, pela autoridade competente, do grau de sigilo dado à informação, documento, material, área ou instalação;

**c) Controle de Acesso:** Conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

**d) Correio Eletrônico:** Método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;

**e) Dado:** Representação de uma informação, instrução ou conceito, de modo que possa ser armazenado e processado por um computador;

**f) Dispositivos Removíveis de Armazenamento de Informação**: Dispositivos que podem armazenar informações e serem removidos do equipamento, permitindo a portabilidade dos dados, como CDs, DVDs e pen drives;

**g) Estação de Trabalho:** Dispositivo utilizado por um colaborador para executar tarefas relacionadas às suas funções na **PREFEITURA**, incluindo desktops, laptops e terminais;

**h) Incidente de Segurança:** Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

**i ) *Peer-to-peer* (P2P):** Permite conectar o computador de um usuário a outro para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, entre outros;

**j) Recursos de Tecnologia da Informação e Comunicação ou simplesmente "Recursos de TIC":** Ativos de hardware, software, serviços de conexão e comunicação ou infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações;

**k) Segurança da Informação:** Preservação da confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação. Visa proteger a informação contra ameaças para garantir a continuidade dos negócios, minimizar danos e maximizar o retorno sobre investimentos e novas oportunidades de transação;

**l) Servidor de Rede:** Recurso de TIC com a finalidade de disponibilizar ou gerenciar serviços ou sistemas de informação;

**m) Usuário:** Servidores públicos municipais, cargos comissionados, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da **PREFEITURA**, solicitada via ofício e formalizada por meio da assinatura do Termo de Responsabilidade;

**n) VPN (*Virtual Private Network*):** Rede de dados privada que faz uso das infraestruturas públicas de telecomunicações, preservando a privacidade, sendo a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas. Com uma VPN, pode-se enviar dados entre dois computadores através de uma rede compartilhada ou pública de uma maneira que emula uma conexão ponto a ponto privada.

**5 DIRETRIZES**

São diretrizes de Segurança da Informação no âmbito da **PREFEITURA**:

**a)** Todos os mecanismos de proteção empregados para garantir a segurança da informação devem ser mantidos a fim de assegurar o princípio da continuidade na Instituição;

**b)** Qualquer informação gerada pelos colaboradores, utilizando total ou parcialmente recursos da **PREFEITURA**, é propriedade da instituição;

**c)** As ameaças e riscos devem ser periodicamente reavaliados para garantir a efetiva proteção da Instituição;

**d)** O acesso às informações produzidas ou recebidas pelas Secretarias/Departamentos Municipais deve ser restrito às atribuições necessárias para o desempenho das atividades correspondentes por parte dos usuários/colaboradores;

**e)** Os processos de aquisição ou contratação de bens e serviços de tecnologia da informação devem estar alinhados com esta PSI e seus documentos auxiliares, em conformidade com a legislação vigente;

**f)** Os equipamentos de informática e comunicação, sistemas e informações devem ser utilizados exclusivamente para o cumprimento das atividades profissionais;

**g)** Esta PSI pode ser revisada periodicamente e, se necessário, ajustada sempre que ocorrerem eventos ou fatos relevantes;

**h)** Os colaboradores devem evitar a circulação de informações e/ou mídias consideradas confidenciais e/ou restritas, bem como devem garantir que não haja relatórios deixados em impressoras ou mídias em locais de fácil acesso;

**i)** Devem aderir ao conceito de "mesa limpa", ou seja, ao concluir o trabalho, garantir que não haja nenhum relatório e/ou mídia confidencial e/ou restrita sobre suas mesas;

**j)** Os procedimentos de gestão de Continuidade do Negócio devem ser executados em conformidade com os requisitos de segurança da informação da Prefeitura.

## 6 REGRAS GERAIS

### 6.1 Controle de Acesso

#### 6.1.1 Conta de Acesso

**6.1.1.1** A conta de acesso na rede da **PREFEITURA** é exclusiva e intransferível, e sua divulgação é estritamente proibida.

**6.1.1.2** O usuário é integralmente responsável por todas as atividades realizadas com sua identificação e senha de acesso.

#### 6.1.2 Segurança da Senha

As senhas dos usuários comuns devem seguir critérios mínimos:

**a)** Mínimo de 8 (oito) caracteres, incluindo letras e números;

**b)** Não repetir as duas últimas senhas utilizadas;

**c)** Troca de senha no primeiro acesso.

#### 6.1.3 Acesso aos Serviços de TI

**6.1.3.1** O acesso aos serviços de TI é concedido apenas a colaboradores autorizados pelas Secretarias.

**6.1.3.2** Qualquer anormalidade no acesso deve ser reportada imediatamente a Tecnologia da Informação (TI).

#### 6.1.4 Controle de Acesso Físico

**6.1.4.1** Os controles de acesso físico visam restringir o acesso não autorizado a dados e arquivos relacionados às atividades da **PREFEITURA**.

**6.1.4.2** O acesso as áreas internas são permitidas somente a pessoas autorizadas.

### 6.2 Uso da Internet

#### 6.2.1 Restrição de Conteúdo

**6.2.1.1** O acesso à Internet deve limitar-se a fins profissionais, relacionados às atividades institucionais.

**6.2.1.2** Cada usuário é responsável pelas ações e acessos realizados através de sua conta de acesso.

#### 6.2.2 Propriedade e Controle de Acesso

**6.2.2.1** Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são propriedade da instituição.

**6.2.2.2** A instituição reserva-se o direito de analisar e, se necessário, bloquear arquivos, sites, correios

eletrônicos, domínios ou aplicativos na rede/internet, a fim de garantir o cumprimento desta Política de Segurança da Informação;

**6.2.3 Restrições de Acesso**

**6.2.3.1** É proibido acessar conteúdos ofensivos, ilegais ou impróprios, incluindo pornografia, pedofilia, preconceitos, vandalismo, entre outros.

**6.2.3.2** Não é permitido o uso recreativo da internet durante o horário de expediente.

**6.2.3.3** O uso de proxies anônimos, VPNs, e tuteladores, assim como o acesso a rádio, TV em tempo real, jogos, e outros conteúdos não relacionados ao trabalho são estritamente proibidos.

**6.2.4 Bloqueios**

A instituição poderá bloquear o acesso a arquivos e sites não autorizados que comprometam o desempenho da rede ou a produtividade do colaborador, além de expor a rede a riscos de segurança.

**6.2.5 Consequências da Utilização Irregular**

**6.2.5.1** Em caso de utilização irregular, o usuário poderá ter seu acesso à Internet bloqueado, sendo comunicado à sua chefia imediata.

**6.2.5.2** O envolvimento em práticas irregulares pode resultar em processo administrativo disciplinar e nas sanções legais aplicáveis, garantindo-se o direito ao contraditório e à ampla defesa.

**6.3 Uso de Recursos de Computacionais**

**6.3.1** Os recursos computacionais devem ser exclusivamente utilizados para a execução de atividades relacionadas aos interesses da **PREFEITURA**.

**6.3.2** Cada estação de trabalho possui um controle de IP (Protocolo Internet) que a identifica na rede. Portanto, todas as atividades realizadas na estação de trabalho são de responsabilidade do usuário. É fundamental que o usuário faça o *logoff* ou bloqueie a estação de trabalho ao se ausentar do ambiente de trabalho.

**6.3.3** Arquivos armazenados em diretórios temporários (pastas públicas) podem ser acessados por todos os usuários da rede local, o que não garante sua integridade e pode resultar em alterações ou exclusões não autorizadas.

**6.3.4** É proibida a abertura física dos computadores para qualquer finalidade. Caso seja necessário realizar reparos, estes devem ser encaminhados ao setor de Tecnologia da Informação.

**6.3.5** Em caso de dano, inutilização ou extravio de equipamentos, o colaborador deve comunicar imediatamente ao setor de patrimônio, que tomará as providências necessárias.

**6.3.6** É proibido realizar alterações físicas nos equipamentos de informática.

**6.3.7** O colaborador deve zelar pela integridade do equipamento e de seus acessórios, tratando-os estritamente como instrumentos de trabalho.

**6.3.8** Não é permitido alterar as configurações de rede e da BIOS (*Basic Input/Output System*) das máquinas, nem fazer modificações que possam resultar em problemas futuros.

**6.3.9** Não é permitido retirar ou transportar equipamentos de informática da **PREFEITURA** sem autorização prévia do secretário da pasta.

**6.3.10** É proibido o uso não autorizado de equipamentos de informática por pessoas sem vínculo com a **PREFEITURA**.

**6.3.11** É vedado retirar ou danificar placas identificadoras de patrimônio, travas e lacres de segurança dos equipamentos de informática.

**6.4 Uso de E-mail Corporativo**

**6.4.1** O colaborador, a critério de seu chefe imediato e de acordo com as necessidades de serviço e recomendações, poderá ter acesso a uma conta de e-mail oficial, sendo solicitado ao departamento de Tecnologia da Informação (TI).

**6.4.2** O acesso ao serviço de e-mail é protegido por uma senha pessoal e intransferível, sendo proibida sua

divulgação.

**6.4.3** É proibido ao usuário utilizar o serviço de e-mail corporativo com as seguintes finalidades:

**a)** Praticar crimes e infrações de qualquer natureza;

**b)** Realizar ações prejudiciais contra os recursos computacionais da **PREFEITURA** ou de redes externas;

**c)** Distribuir conteúdo obsceno, pornográfico, ofensivo, preconceituoso, discriminatório ou ilegal;

**d)** Enviar anúncios publicitários, mensagens de entretenimento, mensagens de corrente, vírus ou qualquer outro programa de computador que não esteja relacionado com as funções institucionais;

**e)** Compartilhar arquivos de áudio, vídeo ou animações, exceto aqueles relacionados com as atividades institucionais da **PREFEITURA**;

**f)** Realizar outras atividades prejudiciais que possam comprometer a privacidade dos usuários, a segurança do sistema ou a imagem da instituição.

**6.4.4 É responsabilidade do usuário do e-mail corporativo:**

**a)** Manter a senha de acesso ao e-mail em sigilo;

**b)** Fechar o sistema de e-mail (navegador/*browser*) ao se ausentar para evitar acessos não autorizados;

**c)** Gerenciar regularmente a caixa de entrada do e-mail, evitando exceder o limite de armazenamento e garantindo o funcionamento contínuo.

**6.5 *Backups***

**6.5.1** Não será realizado *backup* dos arquivos criados nas estações de trabalho dos colaboradores. Cada usuário é responsável por fazer *backup* de seus arquivos locais e por gerenciar o armazenamento, evitando acumulação desnecessária de dados.

**6.5.2** Cada usuário é responsável pelo armazenamento dos arquivos relacionados à sua unidade no servidor, garantindo assim a realização do *backup* deles.

**6.5.3** É responsabilidade do usuário manter organizado o diretório ao qual tem acesso, evitando o acúmulo de arquivos duplicados e desordenados.

**6.6 Classificação da Informação**

**6.6.1** É responsabilidade do responsável de cada pasta estabelecer critérios relacionados ao nível de confidencialidade das informações (relatórios e/ou mídias) geradas por sua área, conforme a seguinte tabela:

**a) Pública:** Engloba informações acessíveis a usuários da instituição, clientes, fornecedores, prestadores de serviços e público em geral;

**b) Interna:** Abrange informações acessíveis somente aos funcionários da instituição, caracterizadas por um grau de confidencialidade que pode afetar a imagem da organização;

**c) Confidencial:** Compreende informações acessíveis aos usuários da instituição e aos parceiros da organização. A divulgação não autorizada dessas informações pode causar impacto financeiro, de imagem ou operacional no negócio da organização ou do parceiro;

**d) Restrita:** Refere-se a informações acessíveis apenas aos usuários da instituição explicitamente indicados pelo nome ou pela área a que pertencem. A divulgação não autorizada dessas informações pode ocasionar danos significativos ao negócio e/ou comprometer a estratégia empresarial da organização.

**7 PAPÉIS E RESPONSABILIDADES**

**7.1 Alta Direção:**

**a)** Assegurar o cumprimento desta PSI e demais documentos correlatos por parte de seus colaboradores e prestadores de serviços.

**7.2 Tecnologia da Informação (TI):**

**a)** Promover e incentivar a conscientização sobre segurança da informação e comunicações entre os colaboradores;

**b)** Acompanhar investigações e avaliações de danos resultantes de violações de segurança;

**c)** Propor recursos necessários para a implementação das medidas de segurança da informação e comunicações;

**d)** Realizar estudos sobre novas tecnologias e avaliar seus possíveis impactos na segurança da informação e comunicações;

**e)** Receber, organizar, armazenar e tratar adequadamente informações sobre eventos e incidentes de segurança, informando os gestores pertinentes sobre ações corretivas ou de contingência em cada caso.

**7.2 Secretários e Gestores:**

**a)** Cumprir, fazer cumprir e gerenciar o cumprimento desta PSI, naquilo que for aplicável por parte de seus colaboradores.

**7.3 Recursos Humanos:**

**a)** Divulgar e garantir a ciência dos novos colaboradores ao Estatuto do Servidor [inserir] e Políticas de Segurança e Privacidade, da **PREFEITURA** no momento da contratação.

**7.4 Colaboradores:**

**a)** Proteger ativamente as informações confidenciais da organização, mantendo a confidencialidade, integridade e disponibilidade dos dados a que tenha acesso;

**b)** Seguir rigorosamente as Políticas de Segurança da Informação e Privacidade estabelecidas pela **PREFEITURA**;

**c)** Reportar imediatamente ao Secretário da respectiva pasta quaisquer incidentes de Segurança da Informação, suspeitas de violação ou comportamentos inadequados;

**d)** Participar dos treinamentos e atividades de conscientização em Segurança da Informação e Privacidade para manter-se atualizado sobre as melhores práticas e ameaças emergentes;

**e)** Utilizar apenas os recursos de tecnologia da informação autorizados e não alterar quaisquer medidas de segurança em suas atividades cotidianas.

**8 PENALIDADES**

Qualquer violação as disposições estabelecidas nesta PSI incorrerão na aplicação das penalidades cabíveis previstas no Estatuto do Servidor [inserir] da **PREFEITURA**, cláusulas contratuais e legislação aplicável vigente.

**9 CONTROLE DE VERSIONAMENTO**

| SIGLA | VERSÃO | VIGÊNCIA | RESPONSÁVEL | CONTROLE DAS MODIFICAÇÕES |
|---|---|---|---|---|
| **PSI** | 1.0 | [Inserir data publicação do decreto] | [Inserir responsável pela aprovação] | Primeira versão. |

**10 DISPOSIÇÕES FINAIS**

**10.1** O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as Normas, Políticas e Procedimentos aplicáveis pela **PREFEITURA**.

**10.2** Os casos omissos serão remetidos ao Comitê de Segurança da Informação e Privacidade (CSIP) para avaliação.

**10.3** Qualquer dúvida relativa a esta PSI deve ser encaminhada para o endereço eletrônico [inserir].

**10.4** Esta Política entra em vigor na data de sua instituição por decreto.

**11 ANEXOS**

**ANEXO I –** Termo de Ciência da Política de Segurança da Informação (Pessoa Física - PF)

**ANEXO II –** Termo de Ciência da Política de Segurança da Informação (Pessoa Jurídica - PJ)

Paraguaçu Paulista, na data da assinatura digital.

**ANTONIO TAKASHI SASADA (ANTIAN)**
Prefeito

**EMERSON MARTINS DOS SANTOS**
Respondendo temporariamente pela Chefia de Gabinete do Prefeito

Documento assinado eletronicamente por **Emerson Martins dos Santos**, **Chefe de Gabinete do Prefeito**, em 19/01/2026, às 07:36, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

Documento assinado eletronicamente por **Antonio Takashi Sasada**, **Prefeito**, em 19/01/2026, às 11:15, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

A autenticidade deste documento pode ser conferida no site https://cidades.sei.sp.gov.br/marilia/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0131591** e o código CRC **0645F9B4**.

**Referência:** Processo nº 3535507.414.00007434/2025-11 SEI nº 0131591

**PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA**

MINUTA

# TERMO DE CIÊNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PESSOA FÍSICA - PF)

**Processo SEI**: 3535507.414.00007434/2025-11

**Órgão Público**: PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA

**Tipo de Documento:** Termo de Ciência (Pessoa Física - PF)

**Base Legal**: Decreto Municipal nº 7.454, de 16/01/2026.

Pelo presente instrumento, **[NOME COMPLETO]**, inscrito(a) no CPF sob o nº XXX.XXX.XXX-XX, DECLARA para os devidos fins que tomou conhecimento e compreendeu as disposições previstas na Política de Segurança da Informação, instituída pela **PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA,** inscrita no CNPJ n.º 44.547.305/0001-93, se comprometendo a respeitar, no desempenho de suas obrigações contratualmente constituídas, todos os seus termos, condições e princípios, estando sujeito(a) às responsabilidades cabíveis advindas do descumprimento.

Paraguaçu Paulista, na data da assinatura digital.

**[NOME DO SIGNATÁRIO]**

[Cargo do Signatário]

Documento assinado eletronicamente por **Antonio Takashi Sasada**, **Prefeito**, em 19/01/2026, às 11:15, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

Documento assinado eletronicamente por **Emerson Martins dos Santos**, **Chefe de Gabinete do Prefeito**, em 19/01/2026, às 12:28, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

A autenticidade deste documento pode ser conferida no site https://cidades.sei.sp.gov.br/marilia/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0131594** e o código CRC **5828B197**.

**Referência:** Processo nº 3535507.414.00007434/2025-11 SEI nº 0131594

**PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA**

MINUTA

# TERMO DE CIÊNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PESSOA JURÍDICA - PJ)

**Processo SEI**: 3535507.414.00007434/2025-11

**Órgão Público**: PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA

**Tipo de Documento:** Termo de Ciência (Pessoa Jurídica - PJ)

**Base Legal**: Decreto Municipal nº 7.454, de 16/01/2026.

Pelo presente instrumento, a(o) **[RAZÃO SOCIAL]**, inscrito(a) no CNPJ sob o nº XXX.XXX.XXX-XX, DECLARA para os devidos fins que tomou conhecimento e compreendeu as disposições previstas na Política de Segurança da Informação instituída pela **PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE PARAGUAÇU PAULISTA**, inscrita no CNPJ n.º 44.547.305/0001-93, se comprometendo a respeitar, no desempenho de suas obrigações contratualmente constituídas, todos os seus termos, condições e princípios, estando sujeito(a) às responsabilidades cabíveis advindas do descumprimento.

Paraguaçu Paulista, na data da assinatura digital.

**[NOME DO SIGNATÁRIO]**

[Cargo do Signatário]

Documento assinado eletronicamente por **Antonio Takashi Sasada**, **Prefeito**, em 19/01/2026, às 11:15, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

Documento assinado eletronicamente por **Emerson Martins dos Santos**, **Chefe de Gabinete do Prefeito**, em 19/01/2026, às 12:27, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023 e Decreto Municipal de regulamentação do processo eletrônico.

A autenticidade deste documento pode ser conferida no site https://cidades.sei.sp.gov.br/marilia/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0131595** e o código CRC **A61F9D77**.

**Referência:** Processo nº 3535507.414.00007434/2025-11 SEI nº 0131595