PREFEITURA MUNICIPAL DE LIMEIRA

ESTADO DE SÃO PAULO - BRASIL

DECRETO Nº 344, DE 29 DE DEZEMBRO DE 2025.

MURILO BERBERT AVIGO FÉLIX, Prefeito Municipal de Limeira, Estado de São Paulo,

NO EXERCÍCIO de suas funções, em atenção às disposições legais,

CONSIDERANDO que a proteção dos ativos de informação é condição essencial para a continuidade dos serviços públicos, bem como para a preservação da confidencialidade, integridade e disponibilidade das informações sob a guarda do Município;

CONSIDERANDO que a segurança da informação constitui componente indispensável da governança e da transformação digital da Administração Pública Municipal;

CONSIDERANDO a necessidade de estabelecer diretrizes, responsabilidades e regras mandatórias para o uso e a proteção dos recursos tecnológicos e dos dados, inclusive dados pessoais, em conformidade com a legislação aplicável;

CONSIDERANDO que a Política de Segurança da Informação (PSI) define princípios e diretrizes para classificação da informação, controle de acesso, continuidade e resposta a incidentes, bem como conformidade e responsabilização, e

CONSIDERANDO tudo o que consta da Comunicação Interna nº 21.683/2025,

D E C R E T A:

Art. 1º Fica instituída, no âmbito da Administração Pública Municipal direta e indireta do Município de Limeira, a Política de Segurança da Informação (PSI), nos termos do Anexo I deste Decreto.

Art. 2º A PSI aplica-se a todos os órgãos, secretarias, autarquias, fundações e entidades controladas, direta ou indiretamente, pelo Município, bem como a terceiros que tratem ou processem informações municipais, abrangendo ativos de informação físicos e digitais, independentemente de sua localização.

Art. 3º A PSI estabelece princípios e diretrizes para a proteção dos ativos de informação e para a conformidade legal, observados, no mínimo:

I - classificação da informação;

II - controle de acesso e identidade (menor privilégio);

III - segurança em operações e infraestrutura, incluindo proteção contra códigos maliciosos, backup e continuidade;

IV - gestão de incidentes;

V - conscientização e treinamento.

Art. 4º A Secretaria Municipal de Tecnologia e Eficiência (SMUTE) é a autoridade técnica responsável pela coordenação, implementação, gestão de riscos, gestão de incidentes e monitoramento contínuo da PSI, podendo expedir normas complementares, procedimentos e padrões técnicos.

Art. 5º O Encarregado de Proteção de Dados (DPO), no âmbito de suas atribuições, atuará como canal de comunicação com os titulares e com a Autoridade Nacional de Proteção de Dados (ANPD), apoiando a conformidade com a legislação de proteção de dados pessoais.

Art. 6º Os Gestores de Área devem assegurar o cumprimento da PSI por seus colaboradores e a correta classificação dos ativos sob sua responsabilidade, bem como solicitar, justificar e revisar privilégios de acesso quando necessário.

Art. 7º É dever de todos os servidores, empregados públicos, colaboradores, estagiários e prestadores de serviço cumprir integralmente a PSI e as normas complementares e reportar imediatamente à SMUTE qualquer incidente ou suspeita de violação de segurança da informação.

Art. 8º O descumprimento deste Decreto, da PSI e das normas complementares sujeitará o infrator às medidas disciplinares cabíveis, sem prejuízo de responsabilidades administrativas, civis e penais, conforme a legislação aplicável.

Art. 9º A PSI deverá ser revisada pela SMUTE anualmente ou sempre que houver mudanças relevantes na legislação, na tecnologia ou na estrutura organizacional do Município, devendo a SMUTE promover programa contínuo de treinamento e conscientização em segurança da informação.

Art. 10 Fica instituído o Termo de Responsabilidade e Compromisso para Uso de Recursos de Tecnologia da Informação e Comunicação (TIC), constante do Anexo II deste Decreto, de assinatura obrigatória por todos os usuários internos e terceiros que utilizem, administrem ou tenham acesso a recursos de TIC, sistemas, redes, contas, equipamentos e informações sob a guarda do Município.

§ 1º O Termo deverá ser assinado previamente à concessão de credenciais de acesso e poderá ser formalizado em meio físico ou eletrônico, conforme procedimento definido pela SMUTE.

§ 2º O Termo integra o processo de admissão, movimentação, designação de função, contratação ou credenciamento de terceiros, devendo ser renovado sempre que houver atualização relevante da PSI ou a critério da SMUTE.

§ 3º A assinatura do Termo não exime o signatário do cumprimento integral da PSI, das normas complementares e da legislação aplicável, inclusive as disposições relativas à proteção de dados pessoais.

Art. 11 Este Decreto entrará em vigor na data de sua publicação.

PAÇO MUNICIPAL DE LIMEIRA, aos vinte e nove dias do mês de dezembro do ano de dois mil e vinte e cinco.

MURILO BERBERT AVIGO FÉLIX
Prefeito Municipal

PUBLICADO no Gabinete do Prefeito Municipal de Limeira, aos vinte e nove dias do mês de dezembro do ano de dois mil e vinte e cinco.

VILMA DANIELA LOPES
Chefe de Gabinete

Anexo I

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Secretaria Municipal de Tecnologia e Eficiência (SMUTE)

Prefeitura Municipal de Limeira - Estado de São Paulo

Versão: 1.0 (Consolidada)

Data de Emissão: 28 de Novembro de 2025

Revisão: Anual ou sempre que houver alteração relevante (LGPD, ISO, mudanças tecnológicas).

---

1. INTRODUÇÃO

A Política de Segurança da Informação (PSI) da Prefeitura Municipal de Limeira estabelece as diretrizes e regras mandatórias para a proteção dos ativos de informação sob a guarda do Município, visando garantir a confidencialidade, integridade e disponibilidade das informações, a continuidade dos serviços públicos essenciais e a conformidade com a legislação vigente [1] [2].

1.1. Propósito

O principal propósito desta PSI é definir um conjunto de regras e procedimentos que assegurem a proteção dos ativos de informação contra ameaças, vulnerabilidades e riscos, sejam eles internos ou externos, intencionais ou acidentais. A política visa, em última instância, proteger a imagem, a credibilidade e os dados dos cidadãos perante a sociedade.

1.2. Abrangência

Esta Política aplica-se a todos os órgãos, secretarias, autarquias, fundações e entidades controladas direta ou indiretamente pelo Município de Limeira, bem como a terceiros que tratem ou processem informações municipais (servidores, colaboradores, estagiários, terceirizados, parceiros e prestadores de serviço).

A abrangência inclui todos os ativos de informação, sejam eles físicos (documentos, mídias) ou digitais (sistemas, dados, redes, equipamentos), independentemente de sua localização.

1.3. Princípios Fundamentais

A PSI é fundamentada nos princípios básicos da segurança da informação, conforme as melhores práticas internacionais (ISO/IEC 27001) e a legislação brasileira [3]:

Princípio	Definição	Relevância para a Prefeitura de Limeira
Confidencialidade	Garantia de que a informação é acessível apenas por pessoas, entidades ou processos autorizados.	Proteção de dados pessoais (LGPD) e informações estratégicas ou sigilosas.
Integridade	Manutenção da precisão e completude da informação e dos métodos de processamento.	Garantia da confiabilidade dos dados de arrecadação, sistemas e registros públicos.
Disponibilidade	Garantia de que usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.	Continuidade dos serviços públicos essenciais à população (saúde, segurança, arrecadação).
Autenticidade	Garantia da veracidade da identidade de um usuário, sistema ou da origem de uma informação.	Validação de acessos e transações eletrônicas, prevenindo fraudes.
Legalidade	Garantia de que o tratamento da informação está em conformidade com as leis, regulamentos e obrigações contratuais.	Cumprimento integral da LGPD, da LAI e demais legislações aplicáveis.
Responsabilização	Atribuição clara de papéis e responsabilidades para o tratamento da informação e gestão de riscos.	Governança e prestação de contas sobre o uso e proteção dos dados municipais.

2. GOVERNANÇA E RESPONSABILIDADES

A segurança da informação é uma responsabilidade compartilhada, com papéis e responsabilidades claramente definidos:

Papel	Responsabilidade Principal
Prefeito Municipal	Aprovação formal da Política e alocação de recursos necessários para sua implementação.
Secretaria Municipal de Tecnologia e Eficiência (SMUTE)	Autoridade técnica responsável pela coordenação da segurança, implementação da PSI, gestão de incidentes, gerenciamento de riscos e monitoramento contínuo.
Encarregado de Dados (DPO)	Atuar como canal de comunicação entre o Município, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), garantindo a conformidade com a LGPD.
Gestores de Área	Assegurar que seus colaboradores compreendam e cumpram a PSI. Garantir a classificação correta dos ativos de informação sob sua responsabilidade.
Todos os Colaboradores	Cumprir integralmente a PSI e as normas complementares. Reportar imediatamente qualquer incidente ou suspeita de violação de segurança à SMUTE.- Secretaria Municipal de Tecnologia e Eficiência
Terceirizados/Parceiros	Cumprir as cláusulas contratuais de segurança e proteção de dados, reportando incidentes imediatamente.

3. GESTÃO DE ATIVOS DE INFORMAÇÃO

Todos os ativos de informação devem ser protegidos de acordo com seu valor, sensibilidade e criticidade para o Município.

3.1. Classificação da Informação

A informação deve ser classificada pelo seu proprietário (Gestor de Área) de acordo com o nível de dano que sua divulgação, alteração ou indisponibilidade causaria ao Município ou aos cidadãos. A classificação mínima obrigatória é:

Nível	Descrição	Exemplos
Pública	Informação que pode ser divulgada sem restrições (LAI).	Notícias, dados abertos, informações de contato institucional.
Interna	Informação de uso interno, cuja divulgação não causa dano significativo.	Documentos internos, procedimentos operacionais não sensíveis.
Confidencial	Informação sensível, cuja divulgação não autorizada pode causar dano grave.	Dados pessoais (LGPD), informações financeiras, planos estratégicos.
Restrita	Informação de acesso extremamente limitado, cuja divulgação causa dano crítico.	Senhas mestras, chaves criptográficas, dados de saúde sigilosos.

3.2. Uso Aceitável de Ativos

Os ativos de informação e recursos tecnológicos (computadores, redes, softwares, periféricos) são de propriedade do Município e devem ser utilizados primariamente para fins de trabalho. O uso pessoal incidental é permitido, desde que:

- Não interfira nas atividades laborais.
- Não viole a legislação vigente.
- Não comprometa a segurança, a integridade ou a disponibilidade dos sistemas.
- Não envolva o acesso, download ou distribuição de conteúdo ilegal, ofensivo ou inadequado.

---

4. CONTROLE DE ACESSO E IDENTIDADE

O acesso aos ativos de informação deve ser estritamente controlado e monitorado.

4.1. Controle de Acesso Lógico

- **Princípio do Menor Privilégio:** O acesso aos sistemas e dados deve ser concedido estritamente com base na necessidade de trabalho (*need-to-know*).
- **Senhas Fortes:** É obrigatório o uso de senhas fortes, combinando letras maiúsculas, minúsculas, números e símbolos. A troca de senhas deve ser incentivada periodicamente e obrigatória em caso de suspeita de comprometimento.
- **Autenticação de Múltiplos Fatores (MFA):** O uso de MFA é recomendado para acesso a sistemas críticos.
- **Revisão de Privilégios:** Os privilégios de acesso devem ser revisados periodicamente, especialmente em casos de mudança de função ou desligamento do colaborador.

4.2. Segurança Física e Ambiental

Controles de segurança física devem ser implementados para proteger as instalações onde informações e equipamentos são armazenados, incluindo:

- Controle de acesso físico a salas de servidores e *data centers*.
- Proteção contra incêndio, climatização e monitoramento contínuo.
- Política específica para armários de documentação sensível.

---

5. SEGURANÇA EM OPERAÇÕES E INFRAESTRUTURA

5.1. Proteção contra Códigos Maliciosos (Malware)

É obrigatório o uso de soluções de antivírus e *antimalware* centralizadas e atualizadas em todos os equipamentos do Município. A instalação de *softwares* não autorizados é estritamente proibida.

5.2. Backup e Continuidade Operacional

- **Rotina de Backup:** Devem ser estabelecidas rotinas de *backup* regulares e testadas para todos os dados críticos.
- **Regra 3-2-1:** Os *backups* devem seguir a regra 3-2-1 (três cópias de dados, em dois tipos de mídia diferentes, com uma cópia armazenada fora do local - *off-site*).
- **Planos de Continuidade:** A SMUTE deve manter um **Plano de Continuidade de Negócios (BCP)** e um **Plano de Recuperação de Desastres (DRP)** para garantir a rápida retomada dos serviços críticos após um incidente grave.

5.3. Gerenciamento de Vulnerabilidades

A SMUTE deve realizar varreduras de vulnerabilidade e manter um processo rigoroso de gerenciamento de *patches* para garantir que todos os sistemas operacionais e *softwares* de aplicação estejam atualizados e protegidos contra falhas conhecidas.

5.4. Segurança no Desenvolvimento e Aquisição de Sistemas

Requisitos de segurança devem ser incorporados desde a especificação (*SDLC seguro*). Adoção de padrões e *checklists* de segurança para contratação de serviços e avaliação de fornecedores.

---

6. GESTÃO DE INCIDENTES DE SEGURANÇA

Todo e qualquer evento que possa comprometer a segurança da informação deve ser tratado como um incidente.

6.1. Notificação e Resposta

- **Obrigação de Reportar:** Qualquer colaborador que identifique ou suspeite de um incidente de segurança (ex: perda de equipamento, *e-mail* de *phishing*, acesso não autorizado) deve reportar imediatamente à SMUTE.
- **Plano de Resposta a Incidentes (PRI):** A SMUTE deve manter um PRI documentado, que detalhe os procedimentos para detecção, contenção, erradicação e recuperação de incidentes.

6.2. Tratamento de Violações de Dados Pessoais (LGPD)

Em caso de violação de dados pessoais, o DPO e a SMUTE devem seguir o protocolo de comunicação à ANPD e aos titulares dos dados, conforme exigido pela LGPD (Lei nº 13.709/2018).

---

7. CONFORMIDADE LEGAL E SANÇÕES

7.1. Conformidade com a LGPD e LAI

Esta PSI e todas as normas complementares devem estar em total conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e a Lei de Acesso à Informação (LAI). O tratamento de dados pessoais deve seguir os princípios da necessidade, finalidade, minimização e transparência.

7.2. Sanções Disciplinares

O não cumprimento desta Política e das normas complementares sujeitará o infrator às medidas disciplinares cabíveis, conforme a legislação municipal e as relações de trabalho. A inobservância poderá, dependendo do caso, ensejar sanções administrativas, civis e penais.

---

8. REVISÃO E CONSCIENTIZAÇÃO

8.1. Revisão da PSI

Esta Política deve ser revisada pela SMUTE anualmente ou sempre que houver mudanças significativas na legislação, tecnologia ou estrutura organizacional do Município.

8.2. Treinamento e Conscientização

A SMUTE deve promover um programa contínuo de treinamento e conscientização em segurança da informação para todos os colaboradores, com foco em:

- Uso seguro de *e-mail* e internet.
- Reconhecimento de ataques de *phishing* e engenharia social.
- Boas práticas de senhas e controle de acesso.
- Regras de uso de dispositivos móveis e trabalho remoto.

9. DISPOSIÇÕES FINAIS

Esta Política entra em vigor na data de sua publicação e substitui normas internas conflitantes.

Assinam:

Murilo Berbert Avigo Felix
Prefeito Municipal de Limeira

Roger Willians da Fonseca
Secretário Municipal de Tecnologia e Eficiência

Danilo Marques
Encarregado de Proteção de Dados (DPO)

Siber Eduardo Cintra
Diretor de Tecnologia da Informação

REFERÊNCIAS

[1] Governo Digital - Portal Gov.br. *Modelo de Política de Segurança da Informação.* Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/modelo_politica_seguranca_informacao.pdf [2] ISO/IEC 27001. *Information security management systems.*
[3] Lei nº 13.709/2018.*Lei Geral de Proteção de Dados Pessoais (LGPD).*

Anexo II

TERMO DE RESPONSABILIDADE E COMPROMISSO

Uso de Recursos de Tecnologia da Informação e Comunicação (TIC)

Prefeitura Municipal de Limeira

1. OBJETO E ABRANGÊNCIA

O presente Termo formaliza o compromisso do Servidor/Colaborador com o uso ético, legal e seguro dos recursos de Tecnologia da Informação e Comunicação (TIC) da Prefeitura Municipal de Limeira, em conformidade com a Política de Segurança da Informação (PSI) e demais normas complementares vigentes.

O Termo abrange todos os recursos de TIC, incluindo, mas não se limitando a: computadores, *notebooks*, *tablets*, *smartphones*, redes de dados (cabeada e *wireless*), sistemas de informação, contas de e-mail corporativo, acesso à internet e quaisquer dados ou informações sob a guarda do Município.

2. USO E COMPROMISSOS GERAIS DE SEGURANÇA

O Servidor/Colaborador declara ter ciência e se compromete a cumprir integralmente as seguintes diretrizes:

2.1. Confidencialidade, Integridade e Disponibilidade

a) **Confidencialidade:** Não divulgar, sob nenhuma hipótese, informações classificadas como Confidenciais ou Restritas a pessoas não autorizadas, em conformidade com a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI).

b) **Integridade:** Não alterar, destruir ou manipular dados e informações sem a devida autorização e rastreabilidade.

c) **Uso Aceitável:** Utilizar os recursos de TIC primariamente para fins de trabalho, sendo vedado o acesso, *download* ou distribuição de conteúdo ilegal, ofensivo ou que comprometa a imagem da Administração Pública.

2.2. Senhas e Acesso

a) **Responsabilidade Pessoal:** O acesso aos sistemas é pessoal e intransferível. O Servidor/Colaborador é o único responsável por todas as ações realizadas com seu *login* e senha.

b) **Senhas Fortes:** Utilizar senhas fortes e complexas, conforme as diretrizes da PSI, e jamais compartilhá-las com terceiros.

c) **Bloqueio de Estação:** Bloquear a estação de trabalho sempre que se ausentar, mesmo que por curtos períodos.

2.3. Uso, conservação de equipamentos e proteção contra ameaças

a) **Softwares:** É estritamente proibida a instalação de qualquer software, aplicativo ou programa não autorizado ou não fornecido pela Secretaria Municipal de Tecnologia e Eficiência, visando a manutenção da integridade e segurança dos sistemas.

b) **Malware e Phishing:** Utilizar o e-mail e a internet de forma segura, reportando imediatamente à SMUTE qualquer suspeita de *phishing*, *malware* ou acesso não autorizado.

c) **Zeladoria e Responsabilidade:** O Servidor/Colaborador é responsável pela guarda, conservação e bom uso dos equipamentos de tecnologia (computadores, notebooks, monitores, periféricos, etc.) que lhe forem confiados, tratando-os com o devido cuidado e diligência.

d) **Comunicação de Danos:** Qualquer dano, defeito, perda ou roubo dos equipamentos deve ser imediatamente comunicado à chefia imediata e à Secretaria Municipal de Tecnologia e Eficiência para as devidas providências e registros.

e) **Movimentação e Retirada:** A movimentação, alteração de configuração ou retirada de equipamentos do local de trabalho designado deve ser previamente autorizada e registrada pela Secretaria Municipal de Tecnologia e Eficiência.

f) **Uso Exclusivo:** Os equipamentos são destinados ao uso exclusivo para as atividades laborais da Prefeitura Municipal de Limeira, sendo vedado o uso para fins particulares que comprometam o desempenho, a segurança ou a legalidade.

3. POLÍTICA DE INATIVIDADE DE CONTAS E SISTEMAS

O Servidor/Colaborador reconhece e aceita a política de inatividade de contas, que visa a segurança e a gestão eficiente dos recursos de TIC, conforme os seguintes prazos:

Tipo de Conta/Sistema	**Prazo de Inatividade**	**Ação**	**Consequência**
Sistemas Críticos	Após **30 dias** de inatividade	Inativação/Suspensão da conta	Necessidade de solicitação formal de reativação à SMUTE.
Outros Sistemas e Acesso à Rede	Após **60 ou 90 dias** de inatividade (a critério da SMUTE)	Suspensão da conta	Necessidade de solicitação formal de reativação à SMUTE.
E-mail Corporativo	Após **90 dias** de inatividade	Inativação da conta	A conta não receberá novos e-mails.
E-mail Corporativo	Após **120 dias** de inatividade	**Exclusão Definitiva** da conta	A conta e todo o seu conteúdo serão excluídos, **não podendo ser restaurados**.

4. USO E RESPONSABILIDADE DA ASSINATURA ELETRÔNICA

O Servidor/Colaborador reconhece que a Assinatura Eletrônica possui validade jurídica e se compromete a utilizá-la com a máxima diligência e responsabilidade. (Decreto nº 35 de 26 de janeiro de 2024).

a) **Equivalência Legal:** A Assinatura Eletrônica (seja via sistema 1Doc, Gov.BR, certificado ICP-Brasil ou outros mecanismos adotados pelo Município) tem a mesma validade legal e probatória da assinatura manuscrita, conforme a legislação vigente.

b) **Guarda e Sigilo:** O Servidor/Colaborador é o único responsável pela guarda, sigilo e não compartilhamento de suas credenciais de acesso (senhas, *tokens*, *smartcards*) utilizadas para gerar a Assinatura Eletrônica.

c) **Ato de Vontade:** A utilização da Assinatura Eletrônica em qualquer documento ou transação eletrônica representa a manifestação de vontade e a concordância expressa do Servidor/Colaborador com o conteúdo assinado.

d) **Comunicação de Risco:** Em caso de suspeita de comprometimento, perda ou roubo das credenciais de Assinatura Eletrônica, o Servidor/Colaborador deve comunicar imediatamente a SMUTE e o seu superior hierárquico para o bloqueio imediato.

5. SANÇÕES E DISPOSIÇÕES FINAIS

O Servidor/Colaborador está ciente de que o não cumprimento das disposições deste Termo e da PSI sujeitará o infrator às medidas disciplinares cabíveis, conforme a legislação municipal, sem prejuízo das responsabilidades civis e penais aplicáveis.

Declaro que li, compreendi e concordo com todas as cláusulas e condições estabelecidas neste Termo de Responsabilidade e Compromisso.