MUNICIPIO DE AMERICANA:45781176000166
Assinado de forma digital por MUNICIPIO DE AMERICANA:45781176000166
Dados: 2025.12.19 17:19:07 -03'00'

Edição nº 2.017

DIÁRIO OFICIAL

PREFEITURA MUNICIPAL DE AMERICANA

Sábado, 20 de dezembro de 2025

SECRETARIA DE COMUNICAÇÃO E TECNOLOGIA DA INFORMAÇÃO

ATO I

(PSI) – Política de Segurança da Informação

1.1 Introdução

A Prefeitura Municipal de Americana/SP, no exercício de suas competências administrativas e constitucionais, reconhece que a informação é um ativo estratégico essencial à gestão pública, à transparência e à continuidade dos serviços prestados à população.

Com a crescente digitalização dos processos e a adoção de sistemas eletrônicos de gestão, torna-se imprescindível garantir que as informações institucionais e pessoais sejam tratadas com segurança, confidencialidade, integridade e disponibilidade, prevenindo acessos indevidos, perdas, vazamentos ou qualquer forma de comprometimento.

Esta **Política de Segurança da Informação (PSI)** estabelece diretrizes, princípios e responsabilidades para proteger os ativos informacionais da Prefeitura, assegurando a conformidade com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), com a Lei nº 12.527/2011 (Lei de Acesso à Informação – LAI), com a Lei nº 14.129/2021 (Lei do Governo Digital), e com o Decreto nº 9.637/2018 (Política Nacional de Segurança da Informação – PNSI).

A adoção desta política tem como referência as normas ABNT NBR ISO/IEC 27001:2022 e 27002:2023, o NIST *Cybersecurity* Framework (CSF), o COBIT 2019 e as boas práticas da Estratégia de Governo Digital (EGD), adaptadas à realidade de um município de pequeno porte.

Ao implementar esta política, a Prefeitura busca criar uma cultura organizacional de segurança, garantindo a proteção das informações em todas as suas formas — digitais, impressas ou orais — e fortalecendo a confiança da sociedade nas ações da administração pública.

1.2 Objetivo

O objetivo desta Política de Segurança da Informação é estabelecer as diretrizes gerais e os princípios de governança da informação, visando proteger os ativos informacionais da Prefeitura e assegurar que o tratamento de dados e informações seja realizado de forma segura, ética e em conformidade com as legislações vigentes.

Em especial, esta política tem por finalidade:

I – Proteger as informações da Prefeitura Municipal contra acessos não autorizados, uso indevido, modificação, destruição ou divulgação indevida;

II – Assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações, em conformidade com os princípios da segurança da informação definidos pela ABNT NBR ISO/IEC 27001;

III – Orientar servidores, colaboradores, prestadores de serviço, estagiários e terceiros quanto às práticas adequadas de segurança, uso e proteção de informações e sistemas;

IV – Estabelecer responsabilidades institucionais relacionadas à segurança da informação, incluindo o papel do Gestor de TI, do Encarregado de Dados (DPO) e dos usuários;

V – Integrar a segurança da informação à governança pública, alinhando-se ao Plano Diretor de Tecnologia da Informação (PDTI), ao Plano de Transformação Digital e à Política de Proteção de Dados Pessoais da Prefeitura;

VI – Promover a conformidade com a legislação aplicável, em especial com a LGPD, a LAI, a Lei do Governo Digital e demais normas correlatas;

VII – Fomentar a cultura de segurança e de prevenção de incidentes, por meio de treinamentos, auditorias e revisões periódicas desta política;

VIII – Definir diretrizes para o uso, armazenamento, transmissão, compartilhamento e descarte de informações, garantindo sua proteção em todo o ciclo de vida.

1.3 Abrangência e Escopo

Esta Política aplica-se a todos os órgãos, secretarias, departamentos, autarquias e entidades vinculadas à Prefeitura Municipal de Americana/SP, incluindo:

- Servidores públicos efetivos e comissionados;
- Estagiários e colaboradores terceirizados;
- Prestadores de serviços, consultores e empresas contratadas que tratem informações institucionais ou dados pessoais sob responsabilidade da Prefeitura;
- Sistemas, equipamentos, redes, bancos de dados e demais ativos de informação pertencentes ou sob guarda do Município.

1.4 Base Legal e Referências Normativas

A presente política fundamenta-se nos seguintes instrumentos legais e técnicos:

Legislação Brasileira:

- Constituição Federal de 1988 (arts. 5º, 37 e 216);
- Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI);
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- Lei nº 14.129/2021 – Lei do Governo Digital;
- Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação;
- Decreto nº 10.046/2019 – Compartilhamento de Dados no Poder Público;
- Lei nº 14.063/2020 – Assinaturas Eletrônicas na Administração Pública;
- Marco Civil da Internet – Lei nº 12.965/2014.

Normas e Frameworks Técnicos:

- ABNT NBR ISO/IEC 27001:2022 – Sistema de Gestão da Segurança da Informação (SGSI);
- ABNT NBR ISO/IEC 27002:2023 – Controles de Segurança da Informação;
- ABNT NBR ISO/IEC 27701:2021 – Sistema de Gestão de Privacidade da Informação (PIMS);
- NIST Cybersecurity Framework (EUA) – Estrutura de Gerenciamento de Riscos Cibernéticos;
- COBIT 2019 – Governança e Gestão de TI;
- ITIL 4 – Boas práticas de gestão de serviços de TI.

Capítulo 2
Princípios e Diretrizes de Segurança da Informação

2.1 Princípios Fundamentais

A Política de Segurança da Informação da Prefeitura Municipal de Americana/SP é guiada pelos princípios que norteiam a boa governança da informação, em conformidade com a Constituição Federal, a Lei Geral de Proteção de Dados (LGPD), a Lei de Acesso à Informação (LAI) e as normas internacionais da série ISO/IEC 27000.

Tais princípios orientam todas as ações, decisões e controles relacionados à proteção da informação pública e dos dados pessoais sob guarda do Município.

I – Confidencialidade

Garantir que a informação seja acessada apenas por pessoas, sistemas ou entidades devidamente autorizadas.
➞ Fundamentação: art. 46 da LGPD; controles 5.1.1 e 8.2 da ISO/IEC 27002.

II – Integridade

Assegurar que a informação permaneça exata, completa e não tenha sido alterada de forma indevida, acidental ou maliciosa.
➞ Fundamentação: ISO/IEC 27001, cláusula 6.1.2; art. 6º, VI da LGPD.

III – Disponibilidade

Garantir que a informação e os sistemas que a armazenam estejam acessíveis aos usuários autorizados sempre que necessário, dentro dos níveis de serviço estabelecidos.
➞ Fundamentação: art. 7º da LAI; princípio da continuidade do serviço público.

IV – Autenticidade

Assegurar que a identidade das partes envolvidas no processamento de informação possa ser verificada, e que as informações sejam genuínas.
➞ Fundamentação: Lei nº 14.063/2020 (assinaturas eletrônicas) e ISO/IEC 27002, controle 8.4.

V – Legalidade

Todo tratamento de informação e dado pessoal deve respeitar as leis e regulamentos aplicáveis, especialmente a LGPD e as normas municipais correlatas.
➞ Fundamentação: art. 6º, I e II da LGPD; art. 37 da Constituição Federal.

VI – Ética e Responsabilidade

Servidores e prestadores de serviços devem agir com zelo, lealdade e boa-fé no trato da informação pública e pessoal, mantendo o sigilo quando necessário e respeitando os direitos dos titulares.

➞ Fundamentação: art. 116 da Lei nº 8.112/1990 (aplicável por analogia), e princípios da moralidade e eficiência administrativa.

VII – Transparência e Controle Social

A segurança da informação não deve ser usada como pretexto para restringir o acesso às informações de interesse público.

➞ Fundamentação: art. 5º, XXXIII da Constituição Federal e art. 3º da Lei nº 12.527/2011.

VIII – Responsabilização e Prestação de Contas (Accountability)

Cada servidor, colaborador ou terceiro deve ser responsável pelos atos praticados no tratamento e proteção da informação.

➞ Fundamentação: art. 6º, X da LGPD e art. 8º da Lei nº 14.129/2021 (Governo Digital).

2.2 Diretrizes Gerais de Segurança da Informação

Para assegurar a observância dos princípios acima, esta política estabelece as seguintes diretrizes, aplicáveis a todos os órgãos e entidades da Prefeitura:

Diretriz 1 – Gestão da Informação como Ativo Institucional

Toda informação gerada, recebida ou armazenada pela Prefeitura é considerada ativo público e deve ser protegida conforme sua criticidade e valor para a administração e para a sociedade.

Diretriz 2 – Classificação da Informação

As informações devem ser classificadas quanto ao seu nível de sigilo, valor e impacto em caso de comprometimento, conforme níveis definidos em regulamento específico (por exemplo: pública, restrita, confidencial e sigilosa).

Diretriz 3 – Gestão de Riscos de Segurança

A Prefeitura deverá identificar, avaliar e tratar riscos que possam afetar a segurança da informação, adotando medidas preventivas, corretivas e mitigadoras, compatíveis com sua capacidade operacional e orçamentária.

Diretriz 4 – Conscientização e Capacitação

Todos os servidores, colaboradores e prestadores de serviço devem ser capacitados sobre boas práticas de segurança, privacidade e proteção de dados, com ênfase nas rotinas diárias da administração municipal.

Diretriz 5 – Controle de Acesso e Autenticação

O acesso a sistemas, redes e bancos de dados deverá ser concedido apenas a usuários devidamente autorizados, com base em perfis de acesso definidos e revisados periodicamente.

Diretriz 6 – Continuidade de Negócios

A Prefeitura deve garantir que incidentes ou desastres não comprometam a continuidade dos serviços essenciais, mantendo planos de backup e recuperação regularmente testados.

Diretriz 7 – Gestão de Incidentes de Segurança

Todo incidente de segurança deve ser comunicado imediatamente à unidade de TI e ao Encarregado de Dados, devendo ser registrado, analisado e tratado de acordo com o Plano de Resposta a Incidentes.

Diretriz 8 – Segurança de Terceiros e Contratos

Os contratos com fornecedores e prestadores de serviços que tratem informações ou dados pessoais devem conter cláusulas específicas de confidencialidade, proteção de dados e segurança da informação, incluindo responsabilidades e penalidades.

Diretriz 9 – Auditoria, Monitoramento e Melhoria Contínua

A política e seus controles devem ser auditados periodicamente, com relatórios encaminhados à alta administração, visando à melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI).

Diretriz 10 – Alinhamento com o Governo Digital e a Transparência

As ações de segurança da informação devem estar alinhadas às diretrizes da Lei do Governo Digital (Lei nº 14.129/2021), priorizando soluções tecnológicas seguras, interoperáveis e sustentáveis.

Capítulo 3
Papéis e Responsabilidades

3.1 Princípio da Responsabilidade Compartilhada

A segurança da informação é responsabilidade de todas as pessoas que tratam informações ou utilizam ativos tecnológicos da Prefeitura Municipal de Americana/SP.

Cada agente público, servidor, colaborador ou prestador de serviço é corresponsável pela proteção das informações sob sua guarda, devendo agir com zelo, ética e observância às normas desta Política.

3.2 Alta Administração Municipal

A Alta Administração – composta pelo Prefeito, Secretários Municipais e dirigentes de autarquias e fundações – possui papel estratégico na governança da segurança da informação.

Compete à Alta Administração:

I – Aprovar esta Política de Segurança da Informação e suas revisões;

II – Garantir que a segurança da informação seja tratada como prioridade institucional, integrando-a aos planos estratégicos da Prefeitura;

III – Designar formalmente os responsáveis pela gestão da segurança da informação e pelo tratamento de dados pessoais;

IV – Assegurar que os recursos humanos, técnicos e financeiros necessários à execução da política sejam providos;

V – Acompanhar periodicamente relatórios de auditoria, risco e conformidade em segurança da informação;

VI – Zelar pelo cumprimento das legislações aplicáveis, especialmente a LGPD, a LAI, a Lei do Governo Digital e o Decreto nº 9.637/2018 (PNSI).

3.3 Comitê Municipal de Segurança da Informação e Proteção de Dados

A Prefeitura instituirá, por ato normativo, um Comitê Municipal de Segurança da Informação e Proteção de Dados, de caráter consultivo e deliberativo.

Compete ao Comitê:

I – Propor normas complementares, manuais e planos específicos de segurança da informação;

II – Avaliar e priorizar ações decorrentes de incidentes de segurança e vazamentos de dados;

III – Acompanhar os indicadores de maturidade de segurança e de governança digital;

IV – Promover a integração entre as unidades de Tecnologia da Informação, Controladoria, Procuradoria Geral, Secretaria de Administração e demais órgãos envolvidos;

V – Emitir pareceres sobre contratos, convênios e parcerias que envolvam tratamento de informações sensíveis ou pessoais.

➞ Fundamentação: arts. 50 e 52 da LGPD; Decreto nº 9.637/2018 (PNSI); Lei nº 14.129/2021 (Governo Digital).

3.4 Gestor de Tecnologia da Informação

O Gestor de TI é o responsável técnico pela implementação dos controles de segurança e pela administração dos ativos tecnológicos da Prefeitura.

Compete ao Gestor de TI:

I – Implementar e manter o Sistema de Gestão da Segurança da Informação (SGSI) em conformidade com a ISO/IEC 27001;

II – Executar os planos de backup, contingência e recuperação de desastres;

III – Gerir as permissões de acesso a sistemas e redes, assegurando controle, rastreabilidade e revisão periódica;

IV – Monitorar incidentes e vulnerabilidades, adotando medidas corretivas;

V – Elaborar relatórios técnicos de conformidade e apresentar resultados ao Comitê e à Alta Administração;

VI – Orientar fornecedores e prestadores de serviço sobre requisitos mínimos de segurança;

VII – Apoiar o Encarregado de Dados (DPO) nas análises técnicas relacionadas a incidentes e riscos de privacidade.

3.5 Encarregado pelo Tratamento de Dados Pessoais (DPO)

O Encarregado de Dados, designado conforme o art. 41 da LGPD, atua como canal de comunicação entre o Município, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Compete ao DPO:

I – Orientar servidores e gestores sobre as práticas de tratamento de dados pessoais e segurança da informação;

II – Receber e responder comunicações de titulares e da ANPD;

III – Acompanhar e registrar incidentes de segurança envolvendo dados pessoais;

IV – Coordenar a implementação da Política de Proteção de Dados Pessoais e apoiar o Comitê na revisão desta Política;

V – Elaborar relatórios de impacto à proteção de dados pessoais (RIPD), em articulação com o Gestor de TI;

VI – Zelar pela integração entre as práticas de privacidade (ISO/IEC 27701) e de segurança da informação (ISO/IEC 27001).

3.6 Gestores de Secretarias e Unidades Administrativas

Cada Secretaria ou Unidade Administrativa da Prefeitura é responsável pela proteção das informações sob sua gestão.

Compete aos Gestores:

I – Cumprir e fazer cumprir esta Política em sua unidade;

II – Classificar as informações sob sua responsabilidade conforme níveis de sigilo definidos;

III – Designar, quando necessário, um ponto focal para assuntos de segurança da informação;

IV – Garantir que documentos e sistemas estejam devidamente protegidos física e logicamente;

V – Comunicar imediatamente ao Gestor de TI e ao DPO qualquer incidente ou suspeita de violação de dados;

VI – Promover a conscientização de seus servidores e colaboradores.

3.7 Servidores Públicos, Estagiários e Colaboradores

Todos os usuários dos ativos de informação têm responsabilidades individuais no uso ético, seguro e responsável dos recursos tecnológicos da Prefeitura.

Compete a cada usuário:

I – Cumprir as normas desta Política e das demais políticas correlatas (uso aceitável, senhas, e-mail, backup etc.);

II – Zelar pela confidencialidade de senhas e credenciais de acesso;

III – Não compartilhar dados pessoais ou institucionais sem autorização;

IV – Evitar a instalação de softwares não autorizados ou o uso indevido de equipamentos públicos;

V – Reportar imediatamente quaisquer incidentes, erros ou comportamentos suspeitos;

VI – Participar de capacitações e treinamentos oferecidos sobre segurança e proteção de dados.

➞ Fundamentação: art. 116 da Lei 8.112/1990 (aplicável por analogia); arts. 46 e 50 da LGPD; ISO/IEC 27002, controle 6.3.

3.8 Prestadores de Serviço, Fornecedores e Terceiros

Toda empresa contratada que tenha acesso a dados, sistemas ou informações da Prefeitura deve observar esta Política e as cláusulas contratuais específicas de segurança da informação.

Compete aos terceiros:

I – Cumprir as normas de segurança estabelecidas nos contratos e aditivos;

II – Manter confidencialidade sobre todas as informações a que tiver acesso;

III – Adotar medidas técnicas e administrativas compatíveis com o risco da informação tratada;

IV – Comunicar imediatamente incidentes que envolvam dados ou sistemas do Município;

V – Submeter-se a auditorias e verificações de conformidade, quando solicitadas.

➞ Fundamentação: art. 39 da LGPD; ISO/IEC 27036 – Segurança em Relacionamentos com Fornecedores.

Capítulo 4
Gestão de Riscos da Informação

4.1 Conceito e Finalidade

A Gestão de Riscos da Informação é o processo sistemático de identificar, analisar, avaliar, tratar e monitorar eventos que possam comprometer a confidencialidade, integridade, disponibilidade ou autenticidade das informações da Prefeitura Municipal de Americana/SP.

O objetivo deste processo é reduzir a probabilidade e o impacto de incidentes de segurança, garantindo a continuidade dos serviços públicos, a conformidade legal e a confiança dos cidadãos nos sistemas municipais.

➞ Base normativa:

- ABNT NBR ISO/IEC 27005:2023 – Gestão de Riscos de Segurança da Informação;
- ABNT NBR ISO/IEC 27001:2022 – Cláusula 6.1.2 (Ações para tratar riscos);
- NIST SP 800-37 Rev. 2 e NIST CSF (Identify, Protect, Detect, Respond, Recover);

- Artigos 6º (VII e X) e 46 da LGPD;
- Art. 15 da Lei 14.129/2021 (Lei do Governo Digital).

4.2 Princípios da Gestão de Riscos

A gestão de riscos da informação observará os seguintes princípios:

I – Proporcionalidade: as medidas de controle devem ser compatíveis com o porte do município, a criticidade da informação e a capacidade operacional da Prefeitura.

II – Prevenção: prioriza-se a identificação e mitigação de vulnerabilidades antes da ocorrência de incidentes.

III – Continuidade: os riscos devem ser geridos de forma permanente, como processo cíclico de melhoria contínua.

IV – Responsabilidade Compartilhada: todos os servidores e gestores são corresponsáveis pela identificação e reporte de riscos.

V – Rastreabilidade e Transparência: as decisões e tratamentos de risco devem ser documentados, auditáveis e comunicáveis à Alta Administração.

4.3 Escopo da Gestão de Riscos

A gestão de riscos abrange todos os ativos de informação sob responsabilidade da Prefeitura, incluindo:

- Sistemas corporativos e bancos de dados;
- Equipamentos de informática, redes e servidores;
- Documentos físicos e eletrônicos;
- Dados pessoais e sensíveis tratados por secretarias municipais;
- Processos administrativos que dependem de tecnologia da informação;
- Fornecedores, contratos e terceiros que tratem informações municipais.

4.4 Etapas do Processo de Gestão de Riscos

O processo seguirá o ciclo contínuo previsto na ISO/IEC 27005, adaptado à realidade municipal:

Etapa 1 – Identificação de Ativos e Ameaças

Mapeamento dos ativos de informação e identificação das possíveis ameaças (internas ou externas) que possam comprometer a segurança.

Etapa 2 – Análise de Vulnerabilidades e Impactos

Analisar as vulnerabilidades existentes e os impactos potenciais sobre as operações municipais, classificando-os como baixo, médio ou alto impacto, conforme critérios definidos pelo Comitê de Segurança da Informação.

Etapa 3 – Avaliação de Probabilidade

Avaliar a probabilidade de ocorrência de cada risco com base em histórico de incidentes, nível de exposição e controles existentes.

Etapa 4 – Determinação do Nível de Risco

Combinar probabilidade e impacto para determinar o nível de risco (baixo, moderado, alto ou crítico), utilizando matriz padronizada de risco definida pela unidade de TI.

Etapa 5 – Tratamento do Risco

Definir as ações adequadas:

a) Mitigar: implementar controles que reduzam o risco;

b) Transferir: compartilhar o risco com terceiros (por exemplo, contratos e seguros);

c) Aceitar: aceitar riscos residuais, mediante aprovação da Alta Administração;

d) Evitar: eliminar o risco pela interrupção da atividade que o gera.

Etapa 6 – Monitoramento e Revisão

Monitorar continuamente os riscos, atualizar controles e revisar o plano de gestão conforme mudanças tecnológicas, organizacionais ou legais.

4.5 Responsabilidades pela Gestão de Riscos

I – Alta Administração: aprovar os resultados da avaliação de riscos e prover recursos necessários à mitigação.

II – Comitê Municipal de Segurança da Informação: coordenar o processo de gestão de riscos, revisar a matriz e propor medidas de controle.

III – Gestor de TI: implementar controles técnicos, monitorar vulnerabilidades e manter atualizada a base de ativos.

IV – Encarregado de Dados (DPO): acompanhar os riscos relacionados ao tratamento de dados pessoais e elaborar Relatórios de Impacto à Proteção de Dados (RIPD).

V – Gestores de Secretarias: identificar riscos em processos sob sua responsabilidade e adotar medidas preventivas.

VI – Servidores e Colaboradores: reportar incidentes, irregularidades ou suspeitas que possam indicar vulnerabilidades.

4.6 Integração com Outras Políticas Municipais

A gestão de riscos da informação deve estar alinhada a:

- Plano Diretor de Tecnologia da Informação (PDTI);
- Plano de Continuidade de Negócios (PCN);
- Política de Proteção de Dados Pessoais;
- Plano de Transformação Digital;
- Gestão de Riscos Institucionais (em conformidade com orientações do Tribunal de Contas e da Controladoria).

Essa integração assegura coerência entre a proteção de dados, a segurança da informação e os objetivos estratégicos da Prefeitura.

4.8 Revisão e Melhoria Contínua

O processo de gestão de riscos será revisado anualmente, ou sempre que ocorrerem mudanças significativas na infraestrutura tecnológica, no arcabouço legal ou nos processos administrativos.

As revisões deverão considerar:

- Resultados de auditorias internas e externas;
- Ocorrência de incidentes e falhas identificadas;
- Novas ameaças cibernéticas ou tecnológicas;
- Recomendações de órgãos de controle e da ANPD.

Capítulo 5
Classificação e Tratamento da Informação

5.1 Conceito e Finalidade

A classificação e o tratamento adequado das informações têm como finalidade assegurar a proteção proporcional ao valor, à sensibilidade e ao impacto que o uso, a divulgação, a modificação ou a perda dessas informações possam causar à Prefeitura Municipal de Americana/SP, aos cidadãos ou a terceiros.

Toda informação produzida, recebida, armazenada ou transmitida no âmbito da Prefeitura é considerada ativo informacional público e deve ser protegida conforme seu grau de sigilo, valor estratégico e obrigações legais de guarda.

➞ Base normativa:

- Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI);
- Decreto nº 7.724/2012 – Regulamenta a LAI;
- Lei nº 13.709/2018 – LGPD (arts. 6º, 46 e 50);
- ABNT NBR ISO/IEC 27002:2023 – seção 5.12 (Classificação da Informação);
- Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação (PNSI).

5.2 Princípios de Classificação da Informação

A classificação da informação observará os seguintes princípios:

I – Proporcionalidade: o nível de proteção deve ser compatível com a sensibilidade da informação e o impacto de sua divulgação indevida;

II – Legalidade: a classificação deve respeitar as normas legais sobre transparência, sigilo e proteção de dados pessoais;

III – Temporalidade: as restrições de acesso devem ter prazo definido e revisão periódica;

IV – Rastreabilidade: todo processo de classificação deve ser documentado e identificável quanto à sua origem e responsável;

V – Minimização: apenas as informações estritamente necessárias deverão ser classificadas em níveis restritivos.

5.3 Categorias de Classificação da Informação

As informações sob guarda da Prefeitura Municipal serão classificadas conforme o grau de sigilo e nível de proteção requerido, observando as normas da LAI e do Decreto nº 7.724/2012:

Nível	Denominação	Descrição e Exemplo	Acesso
1. Pública	Informação de livre acesso	Dados e documentos que podem ser divulgados sem restrição. Ex: Relatórios públicos, atas, leis, orçamentos, dados abertos.	Acesso irrestrito.
2. Restrita	Informação interna	Dados cujo acesso é limitado a servidores e gestores da unidade. Ex: memorandos internos, planejamento estratégico, relatórios de TI.	Acesso mediante credencial institucional.
3. Confidencial	Informação sensível ou estratégica	Dados que, se expostos, podem causar danos à segurança institucional, à imagem da administração ou aos interesses públicos. Ex: pareceres jurídicos em andamento, dados financeiros, contratos em fase de licitação.	Acesso restrito a autoridades e servidores autorizados.
4. Sigilosa	Informação classificada em grau de sigilo, conforme LAI	Dados cujo conhecimento não autorizado pode comprometer a segurança da sociedade ou do Estado. Ex: investigações, informações estratégicas, dados de segurança pública.	Acesso controlado e autorizado por autoridade competente, com prazos definidos de restrição (5 a 25 anos).

➞ Observação: o nível “sigiloso” deve ser formalmente designado pela autoridade máxima da Prefeitura, conforme art. 24 a 27 da LAI e art. 31 do Decreto nº 7.724/2012.

5.4 Tratamento da Informação por Natureza

Além do nível de sigilo, o tratamento da informação deve observar sua natureza e finalidade, em especial no que se refere aos dados pessoais e dados sensíveis, conforme a LGPD:

Tipo de Informação	Tratamento Específico
Dados pessoais	Devem ser tratados com base em uma hipótese legal (art. 7º da LGPD), garantindo segurança, confidencialidade e acesso controlado.
Dados pessoais sensíveis	Exigem proteção reforçada (art. 11 da LGPD), com controles adicionais, registro de acesso e medidas de segurança específicas.
Dados de crianças e adolescentes	O tratamento deve respeitar o melhor interesse da criança (art. 14 da LGPD), com consentimento e controles adicionais de sigilo.
Informações públicas	Devem ser publicadas de forma clara, precisa e acessível, observando o princípio da publicidade e o direito de acesso à informação.
Informações estratégicas ou críticas	Devem ter gestão controlada, uso restrito e plano de contingência em caso de incidente.

5.5 Rotulagem e Identificação da Informação

Toda informação classificada como restrita, confidencial ou sigilosa deve ser devidamente rotulada, identificada e protegida.

A rotulagem deverá conter, no mínimo:

- Grau de sigilo (“Restrita”, “Confidencial” ou “Sigilosa”);
- Data da classificação;
- Nome e cargo da autoridade classificadora;
- Prazo de revisão da classificação;
- Unidade responsável pela guarda.

Nos documentos eletrônicos, a classificação deve ser registrada no sistema de gestão documental, com controle de permissões e logs de acesso.

➞ Referência técnica: ISO/IEC 27002, controle 5.13 (Rotulagem de informação).

5.6 Armazenamento e Acesso à Informação

I – O armazenamento das informações deverá ser feito em ambientes seguros, com controle físico e lógico de acesso;

II – Sistemas de informação deverão possuir autenticação individual, criptografia e logs de auditoria;

III – Os acessos devem ser concedidos conforme o princípio do menor privilégio e revisados periodicamente;

IV – Documentos físicos classificados devem ser armazenados em armários trancados, salas seguras ou arquivos com controle de acesso;

V – É vedado o transporte de mídias, *pendrives* ou dispositivos com informações institucionais sem autorização formal.

5.7 Compartilhamento e Transferência de Informações

O compartilhamento interno ou externo de informações deve obedecer às seguintes regras:

I – Ser limitado ao mínimo necessário para a execução da atividade pública;

II – Observar as bases legais previstas no art. 7º e art. 26 da LGPD;

III – Nos casos de compartilhamento com outros entes públicos, observar o Decreto nº 10.046/2019;

IV – No caso de envio de dados a operadores (empresas contratadas), exigir contrato específico contendo cláusulas de sigilo e segurança;

V – Toda transferência de informações deve ser registrada, documentada e, quando possível, criptografada.

5.8 Retenção e Descarte de Informações

O descarte de informações deve ocorrer de forma segura, controlada e documentada, observando a legislação arquivística e de proteção de dados.

I – O prazo de guarda das informações seguirá o Plano de Classificação e a Tabela de Temporalidade Documental do Município;

II – Informações com dados pessoais devem ser eliminadas após o término da finalidade, salvo obrigação legal de guarda;

III – O descarte de documentos físicos deverá ser feito por fragmentação, trituração ou incineração controlada;

IV – O descarte de informações digitais deverá ocorrer por eliminação segura de mídias ou sobrescrição de dados (*wipe*).

➞ Fundamentação: art. 15, III da LGPD; art. 25, §1º da LAI; ISO/IEC 27002, controle 5.14 (Descarte de informações).

5.9 Auditoria e Revisão da Classificação

O Comitê de Segurança da Informação, com apoio da Controladoria e da TI, deverá realizar auditorias periódicas sobre a classificação e o tratamento das informações, verificando:

- Adequação dos níveis de sigilo aplicados;
- Correta rotulagem e armazenamento;
- Conformidade com as legislações aplicáveis;
- Ocorrência de acessos indevidos ou incidentes.

As revisões das classificações deverão ocorrer, no mínimo, a cada 24 meses, ou sempre que houver alteração significativa no contexto, na legislação ou na sensibilidade da informação.

Capítulo 6
Controle de Acesso à Informação e aos Sistemas

6.1 Conceito e Finalidade

O controle de acesso é o conjunto de políticas, procedimentos e mecanismos destinados a garantir que apenas pessoas devidamente autorizadas possam acessar informações, sistemas, redes e ativos tecnológicos da Prefeitura Municipal de Americana/SP.

O objetivo deste capítulo é assegurar a confidencialidade, integridade, disponibilidade e rastreabilidade das informações, prevenindo acessos indevidos, fraudes, vazamentos e incidentes que possam comprometer os dados públicos e pessoais tratados pela administração municipal.

➞ Base normativa:

- Lei nº 13.709/2018 – LGPD (arts. 6º, VII e 46);
- Lei nº 12.527/2011 – LAI (art. 7º);
- ABNT NBR ISO/IEC 27002:2023 – Controles 5.15 a 5.18;
- Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação;
- Lei nº 14.129/2021 – Lei do Governo Digital (art. 15, incisos II e IV).

6.2 Princípios do Controle de Acesso

O controle de acesso da Prefeitura Municipal é regido pelos seguintes princípios:

I – Necessidade de saber (Need to Know): o acesso às informações é concedido somente a quem necessita delas para executar suas atividades;

II – Menor privilégio: cada usuário deve possuir apenas as permissões mínimas indispensáveis ao desempenho de suas funções;

III – Autenticidade e rastreabilidade: toda ação sobre os sistemas deve ser vinculada a um usuário identificado e autenticado;

IV – Segregação de funções: funções críticas devem ser separadas para evitar conflito de interesses ou fraudes;

V – Temporalidade: os acessos devem ser concedidos por prazo determinado, sendo periodicamente revisados e revogados quando cessada a necessidade.

6.3 Perfis e Tipos de Acesso

Os acessos aos sistemas e informações da Prefeitura serão classificados em três categorias principais:

Tipo de Acesso	Descrição	Exemplos de Aplicação
Administrativo	Permite gerenciar sistemas, usuários e configurações.	Gestor de TI, Administrador de Rede, Coordenador de Sistema.
Operacional	Permite executar funções relacionadas à rotina de trabalho, sem modificar configurações críticas.	Servidor de departamento, agente público.
Consulta (Leitura)	Permite visualizar informações sem alterar dados.	Gestores, auditores, controladores internos.

O Gestor de TI deverá manter um cadastro atualizado de perfis de acesso, contendo identificação do usuário, data de criação, tipo de acesso e responsável pela autorização.

6.4 Procedimentos de Concessão e Revogação de Acesso

I – Todo acesso deverá ser solicitado formalmente pelo gestor da unidade e autorizado pela autoridade competente;

II – O Gestor de TI deverá registrar a data de criação e o motivo do acesso concedido;

III – O acesso de usuários desligados, transferidos ou com alteração de função deverá ser imediatamente revogado;

IV – Contas inativas por mais de 90 dias deverão ser bloqueadas;

V – O Comitê de Segurança da Informação deverá revisar trimestralmente os perfis de acesso e as permissões concedidas.

➞ Referência: ISO/IEC 27002:2023, controles 5.16 e 8.2.

6.5 Autenticação de Usuários

A autenticação de usuários deve garantir a identidade de quem acessa os sistemas, utilizando mecanismos de segurança proporcionais ao nível de risco.

I – Requisitos mínimos:

- Utilização obrigatória de login individual e intransferível;
- Senhas com no mínimo 8 caracteres, contendo letras maiúsculas, minúsculas, números e símbolos;
- Troca obrigatória de senha a cada 90 dias;
- Bloqueio automático após 5 tentativas incorretas consecutivas;
- Proibição de reutilização das últimas 3 senhas.

II – Mecanismos complementares (conforme disponibilidade):

- Autenticação multifator (MFA) para acessos administrativos ou sensíveis;
- Tokens ou certificados digitais para assinatura e autenticação de servidores;
- Controle de acesso baseado em grupos ou funções (RBAC – Role Based Access Control).

➞ Referência técnica: ISO/IEC 27002, controle 8.3 (Gestão de credenciais de autenticação).

6.6 Controle de Acesso Físico

I – O acesso físico a áreas que contenham equipamentos críticos (datacenter, servidores, arquivos, armários de backup) será restrito e autorizado pelo Gestor de TI;

II – Visitantes e prestadores de serviço deverão ser acompanhados e registrados em livro ou sistema de controle;

III – Portas e janelas de áreas sensíveis devem permanecer trancadas fora do horário de expediente;

IV – Equipamentos portáteis (notebooks, HDs externos, *pendrives*) devem ser armazenados de forma segura;

V – Deve ser implementado sistema de rastreabilidade de entrada e saída de equipamentos.

➞ Base: ISO/IEC 27002, seção 7 (Segurança física e ambiental).

6.7 Acesso Remoto e Dispositivos Móveis

I – O acesso remoto aos sistemas da Prefeitura será permitido apenas mediante autorização prévia do Gestor de TI;

II – Todo acesso remoto deverá ocorrer por conexão segura (VPN ou canal criptografado);

III – É vedada a utilização de redes públicas não seguras para acesso a informações institucionais;

IV – Equipamentos pessoais só poderão ser utilizados mediante termo de responsabilidade e aprovação formal (BYOD – Bring Your Own Device controlado);

V – Deve ser implementado controle de logs para monitorar acessos remotos e conexões externas.

➞ Referência: ISO/IEC 27002, controles 8.23 e 8.24.

6.8 Registro, Auditoria e Rastreabilidade de Acessos

Todos os acessos a sistemas e informações críticas deverão ser registrados e auditáveis, contemplando:

- Identificação do usuário;
- Data e hora de acesso;
- Sistema ou recurso acessado;
- Ações executadas;
- Resultado (sucesso ou falha).

Esses registros deverão ser:

- Mantidos por prazo mínimo de 12 meses;
- Armazenados de forma protegida contra alterações;
- Analisados periodicamente pelo Gestor de TI e pela Controladoria.

➞ Fundamentação: art. 6º, X da LGPD (responsabilização e prestação de contas); ISO/IEC 27002, controle 8.15.

6.9 Revogação e Suspensão de Acesso

Os acessos deverão ser suspensos ou revogados imediatamente nas seguintes situações:

I – Desligamento, férias ou afastamento do servidor;

II – Término de contrato de prestador de serviço;

III – Alteração de função ou setor;

IV – Constatação de uso indevido, compartilhamento de credenciais ou descumprimento da política;

V – Identificação de incidente de segurança ou violação de dados.

➞ A revogação deverá ser documentada e comunicada ao Comitê de Segurança da Informação.

6.10 Termo de Responsabilidade de Acesso

Todo usuário com acesso aos ativos tecnológicos da Prefeitura deverá assinar Termo de Responsabilidade de Acesso, comprometendo-se a:

- Utilizar os recursos apenas para fins institucionais;
- Manter sigilo sobre senhas e informações;
- Respeitar esta Política e as demais normas complementares;
- Comunicar imediatamente incidentes ou suspeitas de violação.

➞ Este termo deverá ser arquivado pelo setor de Recursos Humanos e revisado anualmente.

Capítulo 7
Segurança Física, Ambiental e de Infraestrutura Tecnológica

7.1 Conceito e Finalidade

A Segurança Física e Ambiental compreende o conjunto de medidas destinadas a proteger os equipamentos, instalações, documentos e ativos tecnológicos da Prefeitura Municipal de Americana/SP contra ameaças físicas, ambientais e tecnológicas que possam comprometer a confidencialidade, integridade e disponibilidade das informações.

O objetivo é minimizar riscos de danos, interrupções ou perdas causadas por acesso físico não autorizado, incêndios, falhas elétricas, inundações, furtos, sabotagem, ou desastres naturais.

➞ Base normativa:

- ABNT NBR ISO/IEC 27002:2023 – Seção 7 (Segurança física e ambiental);
- Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação;
- Lei nº 13.709/2018 – LGPD (art. 46);
- Lei nº 14.129/2021 – Governo Digital (art. 15);
- Instrução Normativa GSI/PR nº 01/2019.

7.2 Princípios de Proteção Física e Ambiental

As medidas de segurança física e ambiental devem observar os seguintes princípios:

I – Prevenção: adotar medidas para evitar o acesso físico indevido e minimizar a probabilidade de incidentes;

II – Detecção: identificar de forma rápida tentativas de intrusão, incêndios, falhas elétricas e outras anomalias;

III – Resposta: possuir procedimentos claros para reagir adequadamente a eventos e restaurar a normalidade;

IV – Continuidade: assegurar que os ambientes e equipamentos essenciais possam ser restabelecidos sem prejuízo ao funcionamento da administração;

V – Proporcionalidade: as medidas devem ser compatíveis com o valor da informação e com a criticidade do serviço prestado.

7.3 Áreas e Instalações Críticas

Consideram-se áreas críticas para a segurança da informação da Prefeitura:

- Sala de servidores e datacenter municipal (se houver);
- Ambientes que abrigam equipamentos de rede, roteadores e switches;
- Arquivos físicos e salas de documentos sigilosos;
- Estações de trabalho de setores sensíveis (como saúde, finanças e recursos humanos);
- Locais de armazenamento de mídias de backup.

➞ Essas áreas deverão ter controle de acesso físico restrito, registro de entrada e saída de pessoas e monitoramento contínuo, conforme sua importância.

7.4 Controle de Acesso Físico

I – O acesso a áreas críticas deve ser permitido somente a servidores e prestadores devidamente autorizados;

II – Visitantes e técnicos externos deverão ser acompanhados por servidor responsável e registrados em livro ou sistema de controle;

III – As portas e janelas das áreas de TI e arquivos devem permanecer trancadas fora do horário de expediente;

IV – As chaves e cartões de acesso devem ter controle formal de entrega, devolução e substituição;

V – Câmeras de vigilância e sistemas de alarme devem ser utilizados quando possível, respeitando a legislação de proteção de dados e privacidade (art. 7º, II da LGPD).

➞ Referência: ISO/IEC 27002, controle 7.4 (Controles de entrada física).

7.5 Proteção de Equipamentos e Instalações

I – Os equipamentos devem estar dispostos em áreas com ventilação adequada, livres de poeira e calor excessivo;

II – Servidores e nobreaks devem estar posicionados em locais secos, sobre plataformas elevadas, para evitar danos por inundação;

III – Os cabos de energia e dados devem ser protegidos e identificados;

IV – Os equipamentos devem estar conectados a sistemas de proteção elétrica (estabilizadores, filtros de linha e nobreaks);

V – O desligamento dos sistemas críticos deve seguir procedimentos formais de desligamento seguro.

➞ Referência: ISO/IEC 27002, controle 7.6 (Proteção de equipamentos).

7.6 Segurança Elétrica e de Climatização

I – Os ambientes de TI devem dispor de sistema de energia ininterrupta (UPS) e de aterramento elétrico adequado;

II – O sistema elétrico deve ser inspecionado periodicamente;

III – A climatização dos ambientes críticos deve manter temperatura entre 18°C e 24°C e umidade relativa entre 45% e 60%, conforme recomendações técnicas;

IV – Equipamentos de ar-condicionado e ventilação devem receber manutenção preventiva;

V – Em caso de falha elétrica ou oscilação de energia, devem existir procedimentos para desligamento controlado dos servidores.

➞ Referência: ISO/IEC 27002, controle 7.7 (Energia elétrica e climatização adequadas).

7.7 Proteção Contra Incêndios, Inundações e Outras Ameaças

I – As áreas críticas deverão possuir extintores adequados ao tipo de risco (CO_2 ou pó químico seco) e sinalização visível de emergência;

II – As instalações devem manter saídas de emergência desobstruídas, iluminação de emergência e plantas de evacuação;

III – É vedado o armazenamento de materiais inflamáveis ou líquidos próximos aos equipamentos de TI;

IV – Equipamentos e documentos importantes devem ser mantidos acima do nível do piso para reduzir riscos de inundação;

V – Os sistemas de backup devem prever cópia externa (off-site) armazenada em local seguro e distante da sede principal.

➞ Referência: ISO/IEC 27002, controles 7.8 e 7.9.

7.8 Transporte e Remoção de Equipamentos

I – Nenhum equipamento, mídia ou ativo de informação poderá ser retirado das dependências da Prefeitura sem autorização formal da autoridade competente;

II – O transporte de notebooks, pendrives ou HDs externos deverá ocorrer mediante Termo de Responsabilidade;

III – As mídias que contiverem dados sensíveis deverão ser criptografadas ou fisicamente protegidas durante o transporte;

IV – Equipamentos desativados deverão ser armazenados de forma segura até o descarte definitivo;

V – A movimentação de equipamentos deve ser registrada pela unidade de TI.

➞ Referência: ISO/IEC 27002, controle 8.26 (Remoção de ativos).

7.9 Proteção de Documentos Físicos

I – Documentos impressos classificados como restritos, confidenciais ou sigilosos devem ser mantidos em armários trancados ou salas seguras;

II – O acesso físico deve ser limitado aos servidores responsáveis pela unidade;
III – É vedado o abandono de documentos sobre mesas, impressoras ou locais de circulação pública;

IV – Impressões sigilosas devem ser retiradas imediatamente após emissão;

V – O descarte deve ser feito por fragmentação, trituração ou incineração controlada.

➞ Referência: ISO/IEC 27002, controle 5.14 (Descarte seguro de informações).

7.10 Limpeza, Manutenção e Suporte de Instalações

I – Empresas terceirizadas responsáveis por limpeza, manutenção predial ou elétrica deve ser supervisionadas durante o acesso a áreas críticas;

II – Tais empresas deverão assinar termos de confidencialidade e segurança;

III – Ferramentas e materiais utilizados deverão ser inspecionados antes e após o serviço;

IV – É proibido o uso de dispositivos pessoais de armazenamento em ambientes restritos;

V – Toda manutenção deverá ser registrada em relatório e arquivada.

➞ Base: ISO/IEC 27002, controle 7.10 (Segurança durante manutenção e suporte).

7.11 Continuidade Operacional e Recuperação de Desastres

I – O Gestor de TI deverá manter um Plano de Continuidade de Negócios (PCN) e um Plano de Recuperação de Desastres (PRD) documentados e testados periodicamente;
II – O plano deve contemplar: cópias de segurança, contatos de emergência, locais alternativos de operação e procedimentos de restauração;

III – Os testes de restauração deverão ocorrer pelo menos uma vez ao ano;

IV – O resultado dos testes deve ser reportado ao Comitê de Segurança da Informação;

V – O PCN e o PRD devem integrar o Plano Diretor de TI e estar alinhados à estratégia da administração municipal.

➞ Base: ISO/IEC 22301 e ISO/IEC 27031.

Capítulo 8
Cópias de Segurança (Backup) e Recuperação de Dados

8.1 Conceito e Finalidade

As cópias de segurança (backups) são medidas essenciais para garantir a disponibilidade e integridade das informações, assegurando que dados e sistemas da Prefeitura Municipal de Americana/SP possam ser restaurados em caso de falhas, exclusões acidentais, incidentes de segurança, ataques cibernéticos ou desastres naturais.

A finalidade deste capítulo é estabelecer diretrizes, responsabilidades e procedimentos padronizados para o planejamento, execução, armazenamento e verificação de backups, bem como a recuperação de informações e sistemas críticos.

➞ Base normativa:

- ABNT NBR ISO/IEC 27002:2023 – controles 8.13 (backup) e 8.14 (recuperação de dados);
- Lei nº 13.709/2018 – LGPD (art. 46, §2º);
- Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação;
- Lei nº 14.129/2021 – Lei do Governo Digital;
- Portaria SGD/ME nº 9.907/2022 – Diretrizes de segurança e privacidade para órgãos públicos.

8.2 Objetivos Específicos

I – Assegurar a recuperação tempestiva de dados e sistemas em caso de falha, sinistro ou incidente de segurança;

II – Minimizar o impacto de interrupções sobre os serviços públicos e atividades administrativas;

III – Garantir a continuidade operacional e a preservação do patrimônio informacional;

IV – Cumprir as obrigações legais de guarda, sigilo e proteção de dados pessoais e sensíveis;

V – Estabelecer a rastreabilidade de todas as cópias e restaurações de dados realizadas.

8.3 Escopo e Abrangência

Esta política de backup aplica-se a todos os sistemas, bancos de dados, documentos eletrônicos e informações institucionais sob responsabilidade da Prefeitura, incluindo:

- Servidores locais e em nuvem;
- Sistemas administrativos e financeiros;
- Sistemas de saúde, educação e assistência social;
- Arquivos eletrônicos e documentos oficiais;
- Bases de dados contendo informações pessoais ou sensíveis;
- Equipamentos e mídias de armazenamento utilizados para backup.

8.4 Tipos de Backup Adotados

A Prefeitura deverá adotar estratégia combinada de backup, conforme a criticidade das informações:

Tipo	Descrição	Aplicação Recomendada
Completo (Full)	Cópia integral de todos os dados selecionados.	Realizado semanalmente em todos os sistemas principais.
Incremental	Cópia apenas dos dados alterados desde o último backup (completo ou incremental).	Realizado diariamente.
Diferencial	Cópia dos dados alterados desde o último backup completo.	Utilizado como redundância de segurança.
Off-site (externo)	Armazenamento de cópia em local físico distinto da sede principal.	Realizado semanalmente.
Em nuvem (Cloud Backup)	Armazenamento criptografado em plataforma segura de nuvem.	Recomendado para sistemas administrativos e financeiros.

➞ Referência: ISO/IEC 27002, controle 8.13 (Backups de informações).

8.5 Periodicidade e Retenção de Backups

I – O backup diário deve contemplar as bases de dados de sistemas operacionais e documentos críticos;

II – O backup semanal completo deve ser realizado para todos os servidores e sistemas principais;

III – O backup mensal consolidado deve ser preservado por, no mínimo, 12 meses;

IV – Backups relacionados a dados fiscais, contábeis e financeiros devem seguir os prazos de guarda determinados por lei (mínimo de 5 anos, conforme legislação tributária);

V – O tempo de retenção dos backups deve respeitar o princípio da minimização da LGPD, eliminando dados pessoais quando cessar a finalidade do tratamento.

8.6 Armazenamento e Proteção das Cópias

I – As cópias de segurança devem ser armazenadas em ambientes fisicamente seguros, com acesso restrito;

II – O local de armazenamento (sala-cofre, datacenter, ou armário seguro) deve ser protegido contra umidade, poeira, calor excessivo e risco elétrico;

III – Deve haver redundância geográfica, com cópia externa armazenada em local físico ou serviço de nuvem distinto da sede principal;

IV – Os arquivos de backup devem ser criptografados e protegidos por senha forte;

V – A guarda das mídias físicas (HDs externos, fitas, pendrives) deve seguir controle de registro, rastreabilidade e assinatura de termo de responsabilidade;

VI – O transporte de mídias entre locais deve ser feito de forma controlada e documentada.

➞ Referência: ISO/IEC 27002, controles 8.13.4 e 8.26.

8.7 Testes de Restauração e Validação

I – Os backups deverão ser testados periodicamente para verificar sua integridade e capacidade de restauração;

II – Os testes devem ocorrer pelo menos uma vez por trimestre;

III – O Gestor de TI deverá manter relatório dos testes realizados, contendo data, sistema testado, resultado e responsável;

IV – Falhas de restauração deverão ser imediatamente comunicadas ao Comitê de Segurança da Informação e ao DPO;

V – A restauração de dados pessoais deverá ser feita de forma controlada, garantindo que somente usuários autorizados tenham acesso.

➞ Referência: ISO/IEC 27002, controle 8.14 (Testes de restauração de dados).

8.8 Responsabilidades

I – Gestor de Tecnologia da Informação:

- Planejar e implementar a rotina de backups;
- Garantir a integridade, rastreabilidade e documentação das cópias;
- Gerenciar o armazenamento, testes e restaurações;
- Reportar periodicamente os resultados ao Comitê de Segurança da Informação.

II – Comitê Municipal de Segurança da Informação:

- Acompanhar o cumprimento das rotinas de backup;
- Definir prioridades de recuperação e níveis de serviço;
- Avaliar riscos e propor melhorias contínuas.

III – Demais Secretarias e Unidades:

- Informar à TI sobre alterações em sistemas, bases de dados ou processos críticos;
- Apoiar o planejamento da recuperação em caso de falha;
- Respeitar as diretrizes sobre guarda e eliminação de dados.

8.9 Recuperação de Dados e Continuidade Operacional

I – Em caso de incidente ou desastre, a recuperação dos dados deverá seguir o Plano de Recuperação de Desastres (PRD) e o Plano de Continuidade de Negócios (PCN);

II – A restauração deverá priorizar sistemas essenciais ao funcionamento da Prefeitura (como contabilidade, folha de pagamento, saúde e arrecadação);

III – Toda restauração deve ser documentada e validada pelo responsável técnico;

IV – Após a restauração, os sistemas deverão ser submetidos a verificação de integridade e funcionalidade;

V – Quando envolver dados pessoais, a operação deverá ser registrada para fins de prestação de contas (accountability), conforme o art. 6º, X da LGPD.

8.10 Eliminação Segura de Backups Antigos

I – Backups fora do prazo de retenção deverão ser eliminados de forma segura e documentada;

II – A exclusão deve impedir a recuperação dos dados por qualquer meio (técnicas de wipe ou destruição física da mídia);

III – Deve ser lavrado termo ou relatório de descarte contendo data, tipo de mídia e responsável técnico;

IV – O descarte deve observar as regras da Política de Descarte de Informações e as exigências da LGPD quanto à eliminação de dados pessoais.

➞ Referência: ISO/IEC 27002, controle 5.14.

Capítulo 9
Gestão de Incidentes de Segurança da Informação

9.1 Conceito e Finalidade

Incidente de segurança da informação é qualquer evento adverso, confirmado ou suspeito, que possa comprometer a confidencialidade, integridade, disponibilidade ou autenticidade das informações, sistemas ou serviços da Prefeitura Municipal de Americana/SP.

A gestão de incidentes tem por finalidade detectar, registrar, analisar e responder rapidamente a esses eventos, reduzindo seus impactos, restaurando a normalidade operacional e promovendo a melhoria contínua dos controles de segurança.

➞ Base normativa:

- LGPD, art. 48 (Comunicação de incidentes à ANPD e aos titulares);
- ABNT NBR ISO/IEC 27035:2023 – Gestão de Incidentes de Segurança da Informação;
- ABNT NBR ISO/IEC 27002:2023 – Controles 8.16 a 8.18;
- Decreto nº 9.637/2018 – PNSI;

- Lei nº 14.129/2021 – Governo Digital.

9.2 Objetivos Específicos

I – Estabelecer um fluxo padronizado para identificação, comunicação e tratamento de incidentes;

II – Minimizar o impacto técnico, jurídico e reputacional decorrente de falhas ou vazamentos;

III – Assegurar a rastreamento e documentação de todos os eventos; IV – Atender às obrigações legais de notificação previstas na LGPD;

V – Promover a cultura de segurança entre servidores, gestores e prestadores de serviço.

9.3 Abrangência

Aplica-se a todos os órgãos, secretarias, departamentos, autarquias e fundações municipais, bem como a todos os servidores, estagiários, terceirizados e fornecedores que tratem informações ou dados pessoais em nome da Prefeitura.

9.4 Exemplos de Incidentes de Segurança

- Perda, roubo ou furto de equipamento contendo dados institucionais;
- Acesso não autorizado a sistemas ou pastas compartilhadas;
- Envio indevido de documentos ou informações sigilosas;
- Infecção por malware, ransomware ou vírus;
- Exclusão ou alteração não intencional de dados;
- Vazamento ou divulgação indevida de dados pessoais;
- Interrupção de serviços críticos ou falha prolongada de sistemas;
- Tentativas de phishing, engenharia social ou fraudes eletrônicas.

9.5 Princípios da Gestão de Incidentes

I – Imediatismo: todo incidente deve ser comunicado assim que detectado;

II – Responsabilidade: cada agente público é responsável por relatar irregularidades observadas;

III – Sigilo: informações sobre incidentes devem ser tratadas de forma confidencial até sua resolução;

IV – Rastreabilidade: todos os registros e decisões devem ser documentados;

V – Aprendizado Contínuo: cada incidente deve gerar lições para aperfeiçoamento dos controles e políticas.

9.6 Fluxo de Gestão de Incidentes

O processo de gestão seguirá as cinco fases preconizadas pela ISO/IEC 27035, adaptadas à realidade municipal:

1. Identificação e Registro

- O usuário que detectar anomalia ou evento suspeito deve comunicar imediatamente à unidade de TI ou ao Encarregado (DPO).
- O Gestor de TI registra o incidente em formulário próprio, contendo: data/hora, descrição, sistema afetado, tipo de dado, pessoa que reportou e ações iniciais.
- O registro deve ser numerado e arquivado em banco de dados ou planilha oficial.

2. Classificação e Análise

- O Gestor de TI e o Comitê de Segurança avaliam a gravidade, a abrangência e o tipo de incidente (baixo, médio, alto ou crítico).
- Quando envolver dados pessoais ou sensíveis, o Encarregado (DPO) participa obrigatoriamente da análise.

3. Resposta e Contenção

- Adotar medidas imediatas para conter o incidente e impedir sua propagação (bloqueio de conta, desconexão de rede, isolamento de equipamento, etc.);
- Registrar todas as ações adotadas e autoridades envolvidas;
- Preservar evidências digitais e logs para eventual investigação.

4. Comunicação e Notificação

- O Encarregado de Dados deve avaliar a necessidade de notificar a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares afetados, conforme o art. 48 da LGPD;
- A notificação deve ser imediata e conter: natureza do incidente, dados afetados, medidas técnicas adotadas e ações corretivas;
- O Comitê de Segurança poderá comunicar outros órgãos competentes (Controladoria, Polícia Civil, Ministério Público, etc.), conforme o caso.

5. Encerramento e Ações Corretivas

- Após a resolução, deve ser elaborado Relatório de Encerramento do Incidente, contendo causa raiz, impactos, medidas preventivas e responsáveis;
- O Comitê de Segurança revisará o caso e proporá ajustes de processo, treinamento ou infraestrutura;
- O relatório será arquivado por mínimo de 5 anos e poderá subsidiar auditorias ou processos administrativos.

9.7 Responsabilidades

I – Gestor de TI:

- Receber, registrar e tratar tecnicamente o incidente;
- Adotar medidas de contenção e restauração de serviços;
- Preservar evidências digitais;
- Emitir relatório técnico e encaminhar ao Comitê.

II – Encarregado de Dados (DPO):

- Analisar o impacto sobre dados pessoais e sensíveis;
- Avaliar a necessidade de notificação à ANPD e aos titulares;
- Documentar o incidente no Relatório de Impacto à Proteção de Dados (RIPD);
- Coordenar a comunicação institucional em caso de vazamento.

III – Comitê Municipal de Segurança da Informação:

- Acompanhar os incidentes registrados;
- Definir prioridades e recursos de resposta;
- Analisar relatórios de encerramento e recomendar melhorias.

IV – Servidores e Usuários:

- Comunicar imediatamente qualquer ocorrência suspeita;
- Não apagar, alterar ou divulgar informações sobre o incidente;
- Cooperar com a equipe de TI e o Comitê na apuração dos fatos.

9.8 Comunicação com a ANPD e Outros Órgãos

Em conformidade com o art. 48 da LGPD, a Prefeitura deverá comunicar a ANPD e os titulares dos dados quando o incidente puder acarretar risco ou dano relevante aos direitos dos titulares.

A notificação deverá conter:

- Descrição do incidente;
- Dados pessoais afetados;
- Medidas de contenção e correção;
- Possíveis riscos e impactos;
- Contatos do Encarregado de Dados.

A Prefeitura também deverá comunicar, quando necessário, a Controladoria, o Ministério Público ou a Polícia Civil, caso haja indícios de crime, dano patrimonial ou violação de sigilo funcional.

9.9 Treinamento e Conscientização

I – Todos os servidores e colaboradores devem receber orientação anual sobre prevenção e comunicação de incidentes;

II – As capacitações devem incluir simulações de ataques cibernéticos, políticas de senhas, engenharia social e boas práticas no uso de e-mail e internet;

III – As lições aprendidas em incidentes reais deverão ser incorporadas aos programas de treinamento e aos procedimentos operacionais padrão (POPs).

9.10 Documentação e Auditoria

I – Todos os incidentes, relatórios e notificações deverão ser registrados em sistema ou planilha oficial;

II – Os registros devem ser preservados por prazo mínimo de 5 anos;

III – O Comitê de Segurança deverá realizar auditorias anuais sobre o processo de gestão de incidentes;

IV – Os resultados serão encaminhados à Alta Administração e à Controladoria Interna.

Capítulo 10
Treinamento, Conscientização e Cultura de Segurança

10.1 Conceito e Finalidade

A conscientização e a capacitação em segurança da informação são pilares fundamentais para garantir que os servidores públicos, colaboradores e prestadores de serviço compreendam suas responsabilidades e adotem comportamentos seguros e éticos no tratamento de dados e informações públicas.

Este capítulo tem por finalidade instituir diretrizes e mecanismos permanentes de treinamento e educação voltados à segurança da informação e à proteção de dados pessoais, criando uma cultura organizacional de segurança em toda a Prefeitura Municipal de Americana/SP.

➞ Base normativa:

- Lei nº 13.709/2018 – LGPD (arts. 46 e 50);
- Lei nº 14.129/2021 – Lei do Governo Digital (art. 15, incisos IV e V);
- Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação;
- ABNT NBR ISO/IEC 27002:2023 – controles 6.3 e 6.4 (Conscientização, educação e treinamento em segurança da informação).

10.2 Objetivos

I – Promover o entendimento institucional sobre os princípios e boas práticas de segurança da informação;

II – Sensibilizar servidores e terceiros quanto à importância da proteção de dados pessoais e sigilosos;

III – Reduzir a probabilidade de incidentes causados por erro humano ou negligência;

IV – Disseminar orientações sobre uso ético e responsável de recursos tecnológicos;

V – Estimular a participação ativa dos servidores na prevenção, identificação e reporte de incidentes;

VI – Cumprir o dever de adoção de medidas administrativas preventivas exigido pelo art. 46 da LGPD.

10.3 Princípios de Conscientização

Os programas de conscientização deverão seguir os seguintes princípios:

1. Periodicidade: as ações devem ser contínuas e planejadas, não se limitando a eventos pontuais;

2. Acessibilidade: o conteúdo deve ser claro, compreensível e adequado ao perfil dos públicos (administrativo, técnico e operacional);

3. Relevância: os temas devem abordar situações reais e riscos concretos vivenciados pela administração pública;

4. Praticidade: devem incluir exemplos, casos reais e orientações aplicáveis à rotina de trabalho;

5. Evidência e registro: toda ação de treinamento deve ser documentada, registrando data, conteúdo, instrutor e participantes.

10.4 Públicos-Alvo

A política de conscientização abrangerá os seguintes grupos:

Público-Alvo	Conteúdo Focado
Servidores efetivos e comissionados	Princípios da LGPD, sigilo funcional, uso ético de sistemas, identificação de ameaças e boas práticas digitais.
Estagiários e terceirizados	Condutas básicas de segurança, acesso controlado e confidencialidade de informações.
Gestores e secretários	Governança da informação, gestão de riscos, incidentes e responsabilidades administrativas.
Prestadores de serviços de TI	Segurança de redes, backups, incidentes cibernéticos e cláusulas contratuais de confidencialidade.
DPO (Encarregado de Dados) e Comitê	Atualização legal, relatórios de impacto e procedimentos de notificação à ANPD.

10.5 Temas Prioritários de Treinamento

Os programas de capacitação em segurança da informação e proteção de dados deverão abranger, no mínimo, os seguintes temas:

1. Fundamentos da Segurança da Informação (confidencialidade, integridade, disponibilidade e autenticidade);
2. Boas práticas no uso de e-mail, senhas e internet corporativa;
3. Identificação de fraudes digitais, *phishing* e engenharia social;
4. Proteção de dados pessoais e sensíveis (conforme a LGPD);
5. Política de uso de dispositivos móveis e armazenamento em nuvem;

6. Procedimentos em caso de incidentes ou suspeitas de vazamento;
7. Regras de acesso e confidencialidade de informações públicas e restritas;
8. Classificação e descarte seguro de informações;
9. Responsabilidade administrativa e sanções em caso de descumprimento;
10. Ética digital e dever de sigilo funcional.

➞ Referência técnica: ISO/IEC 27002, controle 6.4.

10.6 Formas de Execução e Ferramentas

I – Os treinamentos poderão ser realizados presencialmente ou em formato on-line (EAD), preferencialmente com apoio de vídeos, manuais, cartilhas e plataformas de capacitação;

II – A Secretaria de Administração e o Gestor de TI deverão manter calendário anual de capacitações;

III – Poderão ser utilizadas campanhas temáticas periódicas, como “Mês da Segurança da Informação” ou “Semana da Proteção de Dados”;

IV – A comunicação interna poderá utilizar murais, e-mails, infográficos e avisos eletrônicos com lembretes e boas práticas;

V – O conteúdo deverá ser revisado anualmente, incorporando novas ameaças, legislações e recomendações da ANPD.

10.7 Integração com Programas Municipais

As ações de conscientização deverão estar integradas a outros programas da Prefeitura, tais como:

- Programa de Integridade e Ética Pública;
- Plano Diretor de Tecnologia da Informação (PDTI);
- Política de Proteção de Dados Pessoais;
- Gestão de Riscos Institucionais;
- Capacitações da Escola de Governo Municipal (quando houver).

Essa integração garante coerência entre as políticas de transparência, governança e proteção de dados.

10.8 Responsabilidades

I – Comitê Municipal de Segurança da Informação:

- Planejar e supervisionar as ações de conscientização;
- Propor temas e materiais educativos;
- Avaliar resultados e propor melhorias.

II – Gestor de TI:

- Apoiar tecnicamente as ações de capacitação;
- Incluir conteúdos práticos sobre segurança digital;
- Registrar as evidências de participação e frequência.

III – Encarregado de Dados (DPO):

- Coordenar a capacitação em proteção de dados pessoais;
- Atualizar os conteúdos conforme orientações da ANPD;
- Elaborar relatórios de conformidade com base nas ações realizadas.

IV – Servidores e Colaboradores:

- Participar obrigatoriamente dos treinamentos;
- Aplicar as orientações aprendidas no cotidiano de trabalho;
- Reportar dúvidas ou situações de risco identificadas.

10.9 Registro, Evidências e Auditoria

I – Toda ação de capacitação deverá gerar registro formal contendo data, conteúdo, público-alvo, instrutor e carga horária;

II – Os registros deverão ser arquivados pela Secretaria de Administração ou pelo Comitê de Segurança da Informação;

III – As evidências serão utilizadas para comprovar adoção de medidas preventivas, conforme o art. 46 da LGPD;

IV – A Controladoria Interna poderá auditar as ações de conscientização, verificando a participação e eficácia dos programas.

10.10 Cultura Organizacional de Segurança

A segurança da informação é uma responsabilidade coletiva e contínua. A Prefeitura deve promover uma cultura institucional baseada em:

- Exemplo da liderança: os gestores devem adotar e demonstrar boas práticas;

- Engajamento permanente: os servidores devem compreender que segurança é parte de suas funções;
- Valorização da ética e da transparência: equilíbrio entre proteção e acesso à informação;
- Reconhecimento de boas práticas: estímulo a servidores e equipes que se destacarem na aplicação da política.

➞ Essa cultura deve ser incorporada aos valores institucionais da Prefeitura, consolidando a confiança da sociedade na gestão pública.

Capítulo 11
Auditoria, Monitoramento e Melhoria Contínua

11.1 Conceito e Finalidade

A auditoria e o monitoramento da Política de Segurança da Informação (PSI) têm por objetivo avaliar a conformidade, a eficácia e a aderência das práticas de segurança da Prefeitura Municipal de Americana/SP em relação às diretrizes estabelecidas nesta política e às legislações vigentes.

A melhoria contínua busca garantir que os processos, controles e procedimentos relacionados à segurança da informação evoluam de forma constante, acompanhando as mudanças tecnológicas, legais e organizacionais.

➞ Base normativa:

- ABNT NBR ISO/IEC 27001:2022 – Cláusulas 9.1 a 10.2 (Monitoramento, auditoria e melhoria);
- ABNT NBR ISO/IEC 27002:2023 – Controles 5.35 a 5.37;
- ABNT NBR ISO/IEC 27004:2022 – Avaliação de desempenho da segurança da informação;
- Lei nº 13.709/2018 – LGPD (art. 50 – boas práticas e governança);
- Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação;
- Lei nº 14.129/2021 – Governo Digital (art. 15).

11.2 Objetivos Específicos

I – Avaliar periodicamente a aplicação efetiva das políticas, normas e controles de segurança da informação;

II – Identificar falhas, vulnerabilidades e oportunidades de melhoria;

III – Comprovar a conformidade com a LGPD, a LAI e demais regulamentos aplicáveis;

IV – Fornecer subsídios para a tomada de decisão da Alta Administração e do Comitê de Segurança;

V – Garantir a transparência e a prestação de contas *(accountability*) das ações de segurança da informação;

VI – Manter o ciclo de melhoria contínua (PDCA) ativo: Planejar → Executar → Verificar → Agir.

11.3 Princípios da Auditoria e Monitoramento

A execução das auditorias e do monitoramento deverá respeitar os seguintes princípios:

1. Independência: a auditoria deve ser conduzida de forma imparcial, sem interferência dos auditados;
2. Evidência: as conclusões devem se basear em registros, relatórios e fatos comprováveis;
3. Objetividade: as avaliações devem ser técnicas, fundamentadas e livres de juízo pessoal;
4. Rastreabilidade: todas as constatações e recomendações devem ser documentadas;
5. Transparência: os resultados devem ser compartilhados com a Alta Administração e o Comitê;
6. Periodicidade: o processo deve ocorrer de forma planejada e recorrente.

11.4 Escopo das Auditorias

As auditorias internas e externas deverão abranger, no mínimo, os seguintes aspectos:

- Cumprimento das diretrizes da PSI e políticas complementares (backup, controle de acesso, incidentes etc.);
- Conformidade com as leis e regulamentos aplicáveis (LGPD, LAI, Governo Digital);
- Segurança física e lógica de ambientes e sistemas;
- Controle de acessos e gestão de credenciais;
- Procedimentos de backup, restauração e descarte de dados;

- Registros de incidentes e plano de resposta;
- Conscientização e treinamento de servidores;
- Eficiência das medidas de mitigação de riscos;
- Gestão de contratos e cláusulas de confidencialidade com terceiros.

11.5 Tipos de Auditoria

Tipo	Descrição	Periodicidade Recomendada
Auditoria Interna de Segurança da Informação	Realizada pelo Comitê de Segurança ou pela Controladoria Interna, avaliando o cumprimento das normas e controles internos.	Anualmente.
Auditoria Técnica de TI	Avalia infraestrutura, vulnerabilidades, sistemas, redes, backups e logs. Pode envolver apoio externo.	A cada 12 a 18 meses.
Auditoria de Conformidade LGPD	Verifica a aderência à LGPD, incluindo relatórios de impacto, controles de privacidade e medidas administrativas.	Anualmente ou conforme atualização legal.
Auditoria de Terceiros e Fornecedores	Avalia o cumprimento das cláusulas contratuais de segurança por empresas prestadoras de serviço.	Durante ou após o contrato.

➞ Referência: ISO/IEC 27002, controle 5.35 (Auditoria de segurança da informação).

11.6 Monitoramento Contínuo

I – O Gestor de TI deverá manter mecanismos de monitoramento automatizado para detectar incidentes, falhas ou acessos não autorizados;

II – Logs de acesso e eventos críticos deverão ser revisados periodicamente;

III – O Comitê de Segurança deverá consolidar relatórios semestrais sobre o desempenho da PSI;

IV – Os resultados das auditorias e monitoramentos deverão subsidiar o Plano de Ação e Melhoria Contínua (PAMC) da Prefeitura;

V – O monitoramento deverá considerar indicadores-chave (KPIs), conforme item 11.7.

➞ Referência: ISO/IEC 27002, controle 5.36 (Monitoramento da segurança da informação).

11.7 Indicadores de Desempenho (KPIs)

A eficácia da PSI e dos controles de segurança será avaliada por meio de indicadores mensuráveis, tais como:

Indicador	Descrição	Periodicidade
Taxa de incidentes de segurança	Número de incidentes reportados x mês.	Mensal
Tempo médio de resposta a incidentes	Tempo entre a detecção e a contenção.	Trimestral
Taxa de sucesso de backup/restauração	Percentual de testes de backup bem-sucedidos.	Trimestral
Percentual de servidores treinados	Relação entre servidores capacitados e total de ativos.	Semestral
Nível de conformidade com a LGPD	Grau de aderência às exigências da lei.	Anual
Conclusão de auditorias planejadas	% de auditorias realizadas no período previsto.	Anual

➞ Esses indicadores devem ser acompanhados pelo Comitê e apresentados em relatório anual à Alta Administração.

11.8 Relatórios e Comunicação dos Resultados

I – Os relatórios de auditoria devem conter achados, evidências, recomendações e plano de ação corretivo;

II – O Comitê de Segurança analisará os relatórios e encaminhará à Alta Administração;

III – As recomendações deverão ter prazos e responsáveis designados;

IV – O acompanhamento das correções deverá constar em relatórios de progresso trimestrais;

V – Resultados relevantes podem ser comunicados à Controladoria Interna e ao Tribunal de Contas, quando aplicável.

11.9 Melhoria Contínua (PDCA)

O processo de melhoria contínua da PSI deve seguir o ciclo PDCA (Plan–Do–Check–Act):

1. Planejar (Plan): identificar riscos, definir objetivos e atualizar controles;
2. Executar (Do): implementar políticas, treinamentos e procedimentos;
3. Verificar (Check): monitorar e auditar resultados e conformidade;
4. Agir (Act): corrigir falhas, revisar políticas e promover ajustes.

➞ O ciclo deve ocorrer anualmente, com base nos resultados das auditorias, nos relatórios de incidentes e nos indicadores de desempenho.

11.10 Revisão da Política de Segurança da Informação

I – A PSI deverá ser revisada anualmente ou sempre que houver alterações significativas em leis, tecnologia ou estrutura organizacional;

II – A revisão será coordenada pelo Comitê Municipal de Segurança da Informação, com apoio do Gestor de TI e do Encarregado de Dados (DPO);

III – As versões revisadas deverão ser submetidas à aprovação da Alta Administração Municipal e publicadas no portal institucional;

IV – As alterações devem ser comunicadas a todos os servidores e prestadores de serviço, com treinamento quando necessário.

➞ Referência: ISO/IEC 27002, controle 5.37 (Revisão da política e melhoria contínua).

Capítulo 12
Disposições Finais e Vigência

12.1 Integração com Outras Políticas e Normativos

Esta Política de Segurança da Informação (PSI) integra o conjunto de políticas e normas internas da Prefeitura Municipal de Americana/SP, devendo ser interpretada de forma complementar às seguintes diretrizes e instrumentos institucionais:

I – Política de Proteção de Dados Pessoais, editada em conformidade com a Lei nº 13.709/2018 (LGPD);

II – Plano Diretor de Tecnologia da Informação (PDTI);

III – Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (PRD);

IV – Política de Backup e Recuperação de Dados;

V – Regulamento Interno de Uso de Recursos Tecnológicos e Comunicação Eletrônica;

VI – Código de Ética e Conduta dos Servidores Públicos Municipais;

VII – Demais normas administrativas e regulamentares editadas pela Administração Municipal.

Parágrafo único. Em caso de conflito entre esta política e outros instrumentos internos, prevalecerão as disposições que garantam maior nível de proteção à informação e aos dados pessoais.

12.2 Cumprimento e Fiscalização

I – O cumprimento desta política é obrigatório para todos os servidores públicos, estagiários, colaboradores, prestadores de serviços e fornecedores que, de qualquer forma, tratem informações ou dados sob responsabilidade da Prefeitura;

II – O Comitê Municipal de Segurança da Informação e Proteção de Dados será o órgão responsável por fiscalizar, orientar e propor melhorias contínuas na aplicação desta política;

III – As Secretarias e Unidades Administrativas deverão cooperar com o Comitê, fornecendo informações e relatórios sempre que solicitados;

IV – A Controladoria Interna poderá realizar auditorias específicas para verificar o cumprimento desta política e das normas correlatas.

12.3 Sanções e Responsabilidades

I – O descumprimento das normas estabelecidas nesta política sujeitará o infrator às sanções administrativas, civis e penais previstas em lei, conforme a gravidade da conduta;

II – Configuram infrações, entre outras:

a) acesso ou uso indevido de informações sigilosas;

b) compartilhamento de credenciais, senhas ou chaves de acesso;

c) omissão na comunicação de incidentes;

d) descarte inadequado de documentos ou mídias;

e) negligência no cumprimento das orientações técnicas da área de TI.

III – As penalidades aplicáveis podem incluir:

- advertência;
- suspensão;
- responsabilização civil ou penal, conforme legislação vigente;
- rescisão contratual, no caso de fornecedores e prestadores de serviço.

➞ Fundamentação: art. 46 e 52 da LGPD; art. 116 da Lei nº 8.112/1990 (aplicável por analogia); e Decreto nº 9.637/2018 (PNSI).

12.4 Divulgação e Acesso Público

I – Esta política deverá ser publicada integralmente no portal institucional da Prefeitura e divulgada amplamente entre servidores e colaboradores;

II – A versão atualizada deverá estar disponível para consulta pública, respeitando o princípio da transparência previsto na Lei de Acesso à Informação (Lei nº 12.527/2011);

III – Sempre que revisada, a nova versão deverá ser comunicada formalmente a todas as Secretarias e setores municipais.

12.5 Responsabilidade da Alta Administração

A Alta Administração é responsável por:

I – Garantir o apoio institucional e financeiro necessário à implementação e manutenção das medidas de segurança da informação;

II – Aprovar esta política e suas atualizações;

III – Assegurar a integração da PSI aos instrumentos de planejamento e gestão pública, como o PDTI, o PPA, a LOA e o Plano de Governo Digital.

➞ Base legal: art. 15, incisos I e IV da Lei nº 14.129/2021 (Lei do Governo Digital).

12.6 Revisão e Atualização

I – Esta Política deverá ser revisada anualmente, ou sempre que houver: a) alteração nas legislações aplicáveis (como atualizações da LGPD, ANPD ou normas técnicas);

b) mudanças tecnológicas significativas;

c) recomendações de auditorias internas, externas ou do Tribunal de Contas;

d) incidentes de segurança relevantes que indiquem necessidade de revisão.

II – A revisão será coordenada pelo Comitê Municipal de Segurança da Informação e Proteção de Dados, com apoio da área de Tecnologia da Informação e da Assessoria Jurídica.

III – A versão revisada deverá ser submetida à aprovação da Alta Administração Municipal e registrada formalmente por decreto ou portaria.

12.7 Vigência

I – Esta Política entra em vigor na data de sua aprovação e publicação oficial, passando a integrar o conjunto normativo da Prefeitura Municipal de Americana/SP;

II – Sua aplicação é obrigatória e imediata a todos os servidores, colaboradores e prestadores de serviço vinculados à administração municipal;

III – Ficam revogadas as disposições internas anteriores que tratem de segurança da informação em sentido diverso.

12.8 Disposição Final

A Política de Segurança da Informação da Prefeitura Municipal de Americana/SP tem por finalidade fortalecer a governança pública digital, garantir a continuidade dos serviços, proteger o patrimônio informacional e assegurar o cumprimento dos princípios constitucionais da legalidade, moralidade, eficiência, publicidade e segurança jurídica, promovendo uma administração pública moderna, confiável e transparente.

Americana, 15 de dezembro de 2025

LEON DOMARCO BOTÃO
Secretário de Comunicação e TI

LUCIANA ANDREA CARDOSO
Secretária Adjunta de TI

DIÁRIO OFICIAL

Expediente
Diário Oficial do Município de Americana
www.americana.sp.gov.br

Diagramação
Secretaria de Comunicação e Tecnologia da Informação
Avenida Brasil, 85 - Centro - Americana
E-mail: diario.oficial@americana.sp.gov.br

Administração
Francisco Antônio Sardelli - Prefeito

O conteúdo publicado é de inteira responsabilidade de seus emissores: Órgãos Públicos, Entidades, demais interessados.
Qualquer dúvida ou outra solicitação de errata deverá ser encaminhada diretamente ao órgão emissor.

ATO II

(PSC) PLANO DE CONTINUIDADE DE SERVIÇOS

1. Finalidade

O Plano de Continuidade de Serviços (PCS) tem por objetivo garantir a manutenção ou rápida retomada das atividades essenciais da Prefeitura Municipal em caso de interrupções, incidentes, falhas técnicas, desastres naturais, ataques cibernéticos ou qualquer evento que comprometa a disponibilidade dos serviços públicos.

O PCS assegura a resiliência organizacional, a continuidade das operações críticas e o cumprimento das obrigações legais, minimizando impactos sobre cidadãos, servidores e parceiros institucionais.

2. Base Legal e Normativa

- Lei nº 14.129/2021 (Lei do Governo Digital) – art. 15, incisos II e IV;
- Lei nº 13.709/2018 (LGPD) – art. 46 (segurança e continuidade de dados pessoais);
- Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação;
- ABNT NBR ISO 22301:2020 – Sistema de Gestão da Continuidade de Negócios;
- ABNT NBR ISO/IEC 27031:2022 – Continuidade de serviços de tecnologia da informação;
- Portaria SGD/ME nº 9.907/2022 – Diretrizes de segurança e continuidade para órgãos públicos.
-

3. Escopo

O PCS abrange:

- Todos os órgãos, secretarias, departamentos e autarquias da Prefeitura;
- Sistemas, bancos de dados e serviços digitais essenciais;
- Infraestruturas críticas (datacenter, rede municipal, energia, comunicações);

- Atividades administrativas e operacionais indispensáveis à execução das funções públicas.

4. Objetivos Específicos

I – Proteger as operações críticas da Prefeitura contra interrupções;
II – Assegurar a retomada rápida dos serviços essenciais;
III – Reduzir perdas financeiras, operacionais e reputacionais;
IV – Cumprir as exigências legais de continuidade e segurança da informação;
V – Definir responsabilidades, fluxos e procedimentos de recuperação.

5. Estrutura de Governança

A execução e manutenção do PCS serão coordenadas por:

Função	Responsabilidade
Comitê de Continuidade de Serviços (CCS)	Coordena, aprova e supervisiona o PCS.
Gestor de Tecnologia da Informação (TI)	Implementa medidas de contingência e recuperação dos sistemas.
Encarregado de Dados (DPO)	Garante que os processos de continuidade respeitem a LGPD.
Gestores de Secretarias	Identificam processos críticos e planos alternativos de execução.
Controladoria Interna	Fiscaliza a aplicação do PCS e recomenda melhorias.

6. Identificação dos Serviços Críticos

Os serviços considerados essenciais à continuidade administrativa e social do Município são:

Serviço / Sistema	Órgão Responsável	Impacto da Interrupção	Tempo Máximo de Interrupção Tolerável (RTO)
Gestão de Pessoas – URH/DP - Folha de Pagamento	Secretaria de Administração / RH	Alto	24 horas
Sistema Contábil e Financeiro	Secretaria de Fazenda/Unidade Contábil, Unidade de Gestão Financeira e Unidade de Orçamento.	Alto	24 horas
Sistema de Arrecadação Tributária	Secretaria de Fazenda/Unidade de Gestão Tributária, Unidade de Arrecadação e Unidade de Gestão Financeira	Alto	24 horas
Sistema da Saúde (Prontuários e E-SUS)	Secretaria de Saúde	Alto	12 horas
Sistema Educacional	Secretaria de Educação	Médio	72 horas
Sistema de Protocolo Digital e Documentos	Secretaria de Administração	Médio	48 horas
E-mail Institucional	Secretaria de Comunicação e TI	Médio	48 horas
Portal da Transparência	Secretaria de Comunicação e TI, Controladoria Geral, Comitê de Transparência.	Baixo	72 horas

7. Análise de Riscos e Impactos

Os principais riscos à continuidade dos serviços incluem:

Tipo de Risco	Exemplo	Impacto	Probabilidade	Ação Preventiva
Falha elétrica	Queda de energia na sede	Alto	Média	Nobreaks, gerador e pontos alternativos de energia
Ataque Cibernético	Ransomware ou phishing	Alto	Média	Firewall, antivírus, backup e treinamento de servidores
Desastre natural	Enchente ou incêndio	Alto	Baixa	Cópias off-site e plano de evacuação
Falha de sistema	Erro em servidor ou software	Médio	Alta	Backup diário e redundância de sistemas
Erro humano	Exclusão ou alteração indevida	Médio	Alta	Treinamento e revisão de acessos
Interrupção de internet	Queda de provedor	Médio	Média	Contrato com provedor secundário

8. Estratégias de Continuidade

1. Redundância tecnológica: sistemas críticos hospedados com cópias locais e backup em nuvem;

2. Infraestrutura alternativa: previsão de ponto físico secundário para operação emergencial (ex.: prédio anexo ou escola municipal com rede segura);

3. Procedimentos manuais emergenciais: planilhas e formulários físicos para registros temporários;

4. Comunicação de crise: canal institucional (WhatsApp corporativo, telefone fixo alternativo e e-mail de contingência);

5. Prioridade de restauração: os sistemas da Saúde, Finanças e Administração devem ter prioridade máxima;

6. Equipe de resposta: designar técnicos e gestores para atuar em plantão emergencial durante incidentes.

9. Plano de Ação Imediata (em Situações de Crise)

Fase 1 – Detecção e Avaliação

- Confirmar o incidente ou interrupção;
- Registrar ocorrência em formulário padrão;
- Comunicar o Gestor de TI e o Comitê de Continuidade.

Fase 2 – Resposta e Contenção

- Isolar o problema (sistemas afetados, rede, área física);
- Acionar backup mais recente;
- Implementar plano de contingência operacional.

Fase 3 – Recuperação

- Restaurar sistemas e validar integridade dos dados;
- Retomar gradualmente os serviços essenciais;
- Registrar relatório técnico e comunicar a Alta Administração.

Fase 4 – Pós-Incidente

- Avaliar causas e impactos;
- Atualizar o PCS conforme lições aprendidas;
- Realizar comunicação institucional e registro de auditoria.

10. Comunicação e Notificação

Durante incidentes ou interrupções:

I – A comunicação interna será coordenada pela Secretaria de Administração;

II – A comunicação externa será feita somente por autoridade designada (Prefeito ou Assessoria de Comunicação);

III – Em incidentes com dados pessoais, o DPO deverá avaliar a necessidade de notificação à ANPD e aos titulares, conforme art. 48 da LGPD.

11. Testes e Simulações

I – O PCS deverá ser testado anualmente, com simulações de falhas elétricas, indisponibilidade de rede e perda de dados;

II – Os testes devem ser documentados, registrando resultados, falhas e planos de melhoria;

III – O Comitê de Continuidade revisará o plano com base nas evidências dos testes.

12. Atualização e Melhoria Contínua

I – O PCS deverá ser revisado sempre que ocorrer:

- Mudança de infraestrutura ou de sistemas;
- Alteração de responsabilidades;
- Ocorrência de incidentes reais;
- Atualização legal ou normativa.

II – A revisão será coordenada pelo Comitê de Continuidade, com apoio da TI e da Controladoria.

III – As versões revisadas deverão ser aprovadas pela Alta Administração e publicadas internamente.

13. Vigência

O presente Plano entra em vigor na data de sua aprovação pela Administração Municipal, e deverá ser integrado ao Plano Diretor de Tecnologia da Informação (PDTI) e à Política de Segurança da Informação (PSI), permanecendo em constante atualização e monitoramento.

Americana, 15 de dezembro de 2025

LEON DOMARCO BOTÃO
Secretário de Comunicação e TI

LUCIANA ANDREA CARDOSO
Secretária Adjunta de TI

SECRETARIA DE ADMINISTRAÇÃO

RELAÇÃO DE EXTRATOS

RELAÇÃO DE EXTRATOS DE CONTRATOS, ADITAMENTOS CONTRATUAIS e ATAS DE REGISTRO DE PREÇOS nos quais figuram como contratante a Prefeitura Municipal de Americana, que contém o número do processo administrativo, o nome ou a razão social do contratado, o objeto, a vigência, o valor, a dotação orçamentária (ou base legal da receita) e a data.

GABINETE DO PREFEITO: Cad. 803/25, PE 153/23, PF 7.857/23, Multiway Comércio e Representações Ltda, Quarto Aditamento ao Contrato para a aquisição de produtos e equipamentos e contratação de serviços para expansão de pontos de coleta de imagem e monitoramento, conforme termo de referência. Renovação do prazo e acréscimo de valor (R$ 157.600,08), 12 meses, R$ 2.067.578,40, 02.02.01-3.3.90.39.00, 19-12-2025; SECRETARIA DE ADMINISTRAÇÃO: Cad. 579/25, PE 099/25, PF 5.520/25, R.C.Astolpho - Epp, Ata de Registro de Preços para aquisição de produtos de limpeza para as secretarias municipais e AMERIPREV, 12 meses, 12-12-2025; Cad. 580/25, PE 099/25, PF 5.520/25, Parilimp Com de Prod e Serv de Limpeza Ltda, Ata de Registro de Preços para aquisição de produtos de limpeza para as secretarias municipais e AMERIPREV, 12 meses, 12-12-2025; Cad. 581/25, PE 099/25, PF 5.520/25, C T Bridi Ltda, Ata de Registro de Preços para aquisição de produtos de limpeza para as secretarias municipais e AMERIPREV, 12 meses, 12-12-2025; Cad. 582/25, PE 099/25, PF 5.520/25, Antônio Amaurilio da Silva - Me, Ata de Registro de Preços para aquisição de produtos de limpeza para as secretarias municipais e AMERIPREV, 12 meses, 12-12-2025; Cad. 583/25, PE 099/25, PF 5.520/25, Nova Guaru Limpeza e Utilidades em Geral Ltda, Ata de Registro de Preços para aquisição de produtos de limpeza para as secretarias municipais e AMERIPREV, 12 meses, 12-12-2025; Cad. 584/25, PE 099/25, PF 5.520/25, Pizani Equipamentos de Segurança Ltda, Ata de Registro de Preços para aquisição de produtos de limpeza para as secretarias municipais e AMERIPREV, 12 meses, 12-12-2025; Cad. 585/25, PE 099/25, PF 5.520/25, Luana Baiocchi Gonçalves Ltda, Ata de Registro de Preços para aquisição de produtos de limpeza para as secretarias municipais e AMERIPREV, 12 meses, 12-12-2025; Cad. 586/25, PE 099/25, PF 5.520/25, Arlimed Distribuidora Hospitalar Ltda, Ata de Registro de Preços para aquisição de produtos de limpeza para as secretarias municipais e AMERIPREV, 12 meses, 12-12-2025; Cad. 587/25, PE 099/25, PF 5.520/25, Flexxlimp Comercial Ltda, Ata de Registro de Preços para aquisição de produtos de limpeza para as secretarias municipais e AMERIPREV, 12 meses, 12-12-2025; Cad. 588/25, PE 099/25, PF 5.520/25, Sanmarcos Vassouras e Produtos de Limpeza Ltda, Ata de Registro de Preços para aquisição de produtos de limpeza para as secretarias municipais e AMERIPREV, 12 meses, 12-12-2025; Cad. 589/25, PE 099/25, PF 5.520/25, Low Cost Ltda, Ata de Registro de Preços para aquisição de produtos de limpeza para as secretarias municipais e AMERIPREV, 12 meses, 12-12-2025; Cad. 590/25, PE 099/25, PF 5.520/25, VNLL Participações Ltda, Ata de Registro de Preços para aquisição de produtos de limpeza para as secretarias municipais e AMERIPREV, 12 meses, 12-12-2025; Cad. 591/25, PE 099/25, PF 5.520/25, M.A. Gransoti Batista-Me, Ata de Registro de Preços para aquisição de produtos de limpeza para as secretarias municipais e AMERIPREV, 12 meses, 12-12-2025; Cad. 592/25, PE 099/25, PF 5.520/25, Varrelar Indústria e Comércio Ltda, Ata de Registro de Preços para aquisição de produtos de limpeza para as secretarias municipais e AMERIPREV, 12 meses, 12-12-2025; Cad. 593/25, PE 099/25, PF 5.520/25, G A M Comercial Ltda, Ata de Registro de Preços para aquisição de produtos de limpeza para as secretarias municipais e AMERIPREV, 12 meses, 12-12-2025; Cad. 618/25, PE 135/25, PF 11.564/25, Avox Publicidade Ltda, Ata de Registro de Preços para prestação de serviços de publicação em jornal de grande circulação no Estado de São Paulo e Diário Oficial da União, 12 meses, 18-12-2025; Cad. 619/25, PE 135/25, PF 11.564/25, Gibbor Publicidade e Publicações de Editais Eireli Epp, Ata de Registro de Preços para prestação de serviços de publicação em jornal de grande circulação no Estado de São Paulo e Diário Oficial da União, 12 meses, 18-12-2025; Cad. 775/25, PF 39.889/03, Zanaga Zeitlin Empreendimentos Ltda, Décimo quinto aditamento ao contrato de locação do imóvel Rua Albânia, n°193, Bairro São Domingos II. Renovação do prazo e valor, 12 meses, R$ 1.702,02, 16-12-2025; Cad. 776/25, PF 6.707/10, JDT Administração de Imóveis Ltda, Décimo Terceiro Aditamento ao contrato de locação do imóvel à Rua Padre Manoel da Nóbrega, n° 121, Vila Santa Catarina. Renovação do prazo e valor, 12 meses, R$ 7.161,27, 16-12-2025; Cad. 786/25, PP 002/20, PF 60.911/19, DOC Tecnologia S.A, Sexto Aditamento ao Contrato para prestação de serviço de locação de sistema informatizado integrado oficial de comunicação interna e externa, gestão documental eletrônica e central de atendimento. Regulamentação, nos termos da Lei nº 13.709/2018 (LGPD), da Resolução CD/ANPD nº 18/2024, e da Lei nº 8.666/93, das condições para o tratamento de dados pessoais, 18-12-2025; Cad. 799/25, Inexig. Lic. 013/21, PF 9.368/21, Consorcio Bus Mais, Quinto Aditamento ao Contrato para fornecimento de vales transportes suburbano e intermunicipal da região metropolitana de Campinas aos servidores municipais. Renovação do prazo e valor, 12 meses, R$ 701.164,80, 3.3.90.39.00, 19-12-2025; Cad. 800/25, PF 2.894/21, Empresa Brasileira de Correios e Telégrafos, Sétimo aditamento ao contrato para aquisição de produtos e serviços dos Correios. Acréscimo de valor. Assinado em 03/12/2025, R$ 1.697.500,00, 3.3.90.39.00, 19-12-2025; SECRETARIA DE COMUNICAÇÃO E TECNOLOGIA DA INFORMAÇÃO: Cad. 784/25, PE 137/25, PF 11.376/25, Mapdata - Tecnologia, Informática e Comércio Ltda, Contrato para fornecimento de licenças de software cooperativas Adobe, Coreldraw, com vigência de 24 (vinte e quatro) meses e, Trello por 12 (doze) meses, incluindo suporte técnico e atualizações durante todo o período contratual, 24 meses, R$ 3.405,00, 33.90.40, 18-12-2025; Cad. 785/25, PE 137/25, PF 11.376/25, Solo Network Brasil S.A., Contrato para fornecimento de licenças de software cooperativas Adobe, Coreldraw, com vigência de 24 (vinte e quatro) meses e, Trello por 12 (doze) meses, incluindo suporte técnico e atualizações durante todo o período contratual, 24 meses, R$ 160.071,00, 33.90.40, 18-12-2025; SECRETARIA DE CULTURA E TURISMO: Cad. 779/25, PP 041/21, PF 2.534/21, Faze Comércio de Materiais Hidráulicos Ltda - Me, Quarto Aditamento ao Contrato para prestação de serviços de manutenção preventiva e corretiva dos aparelhos de ar condicionado das unidades da secretaria de cultura. Renovação do prazo e valor, 12 meses, R$ 81.283,61, 02.08.01 - 3.3.90.39.00, 18-12-2025; SECRETARIA DE EDUCAÇÃO: Cad. 620/25, PE 129/25, PF 7.165/25, RCE Artigos de Papelaria - Ltda, Ata de Registro de Preços para aquisição de materiais escolares para atendimento aos alunos das escolas municipais, 12 meses, 18-12-2025; Cad. 621/25, PE 129/25, PF 7.165/25, A.C. de Almeida Informática e Tecnologia Ltda - Me, Ata de Registro de Preços para aquisição de materiais escolares para atendimento aos alunos das escolas municipais, 12 meses, 18-12-2025; Cad. 622/25, PE 129/25, PF 7.165/25, R.C.Astolpho - Epp, Ata de Registro de Preços para aquisição de materiais escolares para atendimento aos alunos das escolas municipais, 12 meses, 18-12-2025; Cad. 623/25, PE 129/25, PF 7.165/25, Atacado Virtual Max Ltda, Ata de Registro de Preços para aquisição de materiais escolares para atendimento aos alunos das escolas municipais, 12 meses, 18-12-2025; Cad. 624/25, PE 129/25, PF 7.165/25, G & L Comércio e Distribuição Ltda, Ata de Registro de Preços para aquisição de materiais escolares para atendimento aos alunos das escolas municipais, 12 meses, 18-12-2025; Cad. 625/25, PE 129/25, PF 7.165/25, 3B Industrial e Comercial Ltda, Ata de Registro de Preços para aquisição de materiais escolares para atendimento aos alunos das escolas municipais, 12 meses, 18-12-2025; Cad. 626/25, PE 129/25, PF 7.165/25, La Luna Comércio de Produtos e Acessórios Ltda, Ata de Registro de Preços para aquisição de materiais escolares para atendimento aos alunos das escolas municipais, 12 meses, 18-12-2025; Cad. 627/25, PE 129/25, PF 7.165/25, JM Suprimentos Ltda, Ata de Registro de Preços para aquisição de materiais escolares para atendimento aos alunos das escolas municipais, 12 meses, 18-12-2025; Cad. 628/25, PE 129/25, PF 7.165/25, 0.011.958 Regiane Freire de Santana, Ata de Registro de Preços para aquisição de materiais escolares para atendimento aos alunos das escolas municipais, 12 meses, 18-12-2025; Cad. 772/25, PE 112/25, PF 6.103/25, RGF Ambiental Ltda, Contrato para prestação de serviços de limpeza em ambiente escolar, incluindo prédios, mobiliários e equipamentos, com disponibilização de mão-de-obra, EPIs, saneantes, domissanitários, materiais e equipamentos, para as escolas da rede municipal de educação de Americana, 12 meses, R$ 6.114.796,80, 02.09.02.33.90.39, 16-12-2025; Cad. 774/25, Disp. Lic. 280/25, PF 3.629/25, Hm Consultoria e Soluções Integradas Ltda, Segundo Aditamento ao Contrato para prestação de serviços técnicos profissionais de cuidador para atuação na rede municipal de ensino como apoio ao processo inclusivo aos alunos matriculados nas unidades escolares de educação infantil (creche e pré-escola), ensino fundamental I e II (anos iniciais e finais). Acréscimo de valor, R$ 184.649,22, 02.09.02 - 3.3.90.39.00, 16-12-2025; Cad. 787/25, Murilo Cassiano Severiano Vicente, Contrato de comodato de bem imóvel, referente à zeladoria da "Casa da Criança Araúna", 48 meses, 18-12-2025; Cad. 788/25, Ch. Pública 005/21, PF 8.507/21, Associação Carlos Benito Franchi, Quarto Aditamento ao Termo de colaboração para execução da Oferta Educacional - segmento Creche. Prorrogação do prazo e reajuste de valor, 12 meses, R$ 1.732.442,88, 02.09.03.3.3.50.39.00.2.034, 18-12-2025; Cad. 789/25, Ch. Pública 005/21, PF 8.507/21, Centro Infanto Ju-

venil de Orientação Progressiva-CIJOP, Quarto Aditamento ao Termo de colaboração para execução da Oferta Educacional - segmento Creche. Prorrogação do prazo e reajuste de valor, 12 meses, R$ 385.801,92, 02.09.03.3.3.50.39.00.2.034, 18-12-2025; Cad. 790/25, Ch. Pública 005/21, PF 8.507/21, Sociedade de Assistência Social de Americana-SASA, Quarto Aditamento ao Termo de colaboração para execução da Oferta Educacional - segmento Creche. Prorrogação do prazo e reajuste de valor, 12 meses, R$ 677.841,84, 02.09.03-3.3.50.39.00.2.034, 18-12-2025; Cad. 791/25, Ch. Pública 005/21, PF 8.507/21, Associação de Promoção e Assistência de Americana-APAM, Quarto Aditamento ao Termo de colaboração para execução da Oferta Educacional - segmento Creche. Prorrogação do prazo e reajuste de valor, 12 meses, R$ 1.441.044,48, 02.09.03.3.3.50.39.00.2.034, 18-12-2025; Cad. 792/25, Ch. Pública 005/21, PF 8.507/21, Fundação Letícia Duarte, Quarto Aditamento ao Termo de colaboração para execução da Oferta Educacional - segmento Creche. Prorrogação do prazo e reajuste de valor, 12 meses, R$ 1.685.134,08, 02.09.03.3.3.50.39.00.2.034.2.034, 18-12-2025; Cad. 793/25, Ch. Pública 005/21, PF 8.507/21, Lar Escola Vó Antonieta, Quarto Aditamento ao Termo de colaboração para execução da Oferta Educacional - segmento Creche. Prorrogação do prazo e reajuste de valor, 12 meses, R$ 1.164.737,28, 02.09.03.3.3.50.39.00.2.034, 18-12-2025; Cad. 794/25, Ch. Pública 005/21, PF 8.507/21, Sociedade de Assistência Social de Americana-SASA, Quarto Aditamento ao Termo de colaboração para execução da Oferta Educacional - segmento Creche. Prorrogação do prazo e reajuste de valor, 12 meses, R$ 781.065,60, 02.09.03.3.3.50.39.00.2.034, 18-12-2025; Cad. 795/25, Ch. Pública 005/21, PF 8.507/21, Centro Infanto Juvenil de Orientação Progressiva-CIJOP, Quinto Aditamento ao Termo de colaboração para execução da Oferta Educacional - segmento Pré Escola. Prorrogação do prazo e reajuste de valor, 12 meses, R$ 567.921,72, 02.09.03.3.3.50.39.00.2.034, 18-12-2025; Cad. 796/25, Ch. Pública 005/21, PF 8.507/21, Vila de São Vicente de Paulo de Americana, Quinto Aditamento ao Termo de colaboração para execução da Oferta Educacional - segmento Creche. Prorrogação do prazo e reajuste de valor, 12 meses, R$ 980.790,72, 02.09.03.3.3.50.39.00.2.034, 18-12-2025; Cad. 797/25, Ch. Pública 005/21, PF 8.507/21, Centro de Orientação Humana São Domingos, Quinto Aditamento ao Termo de colaboração para execução da Oferta Educacional - segmento Creche. Prorrogação do prazo e reajuste de valor, 12 meses, R$ 1.446.459,84, 02.09.03.3.3.50.39.00.2.034, 18-12-2025; Cad. 798/25, Ch. Pública 005/21, PF 8.507/21, Centro de Orientação Humana São Domingos, Quinto Aditamento ao Termo de colaboração para execução da Oferta Educacional - segmento Pré Escola. Prorrogação do prazo e reajuste de valor, 12 meses, R$ 384.721,20, 02.09.03.3.3.50.39.006.2.034, 18-12-2025; SECRETARIA DE MEIO AMBIENTE: Cad. 777/25, PE 075/25, PF 1.780/24, JS Brasilio Estufas Agrícolas Ltda, Primeiro Aditamento ao Contrato para aquisição, com instalação, de estufa agrícola dotada de equipamentos de sustentabilidade. Prorrogação dos prazos, 60 dias, 16-12-2025; SECRETARIA DE OBRAS E SERVIÇOS URBANOS; Cad. 780/25, PP 059/23, PF 12.015/23, Neo Consultoria e Administração de Benefícios Ltda, Segundo Aditamento ao Contrato para prestação de serviços de gerenciamento do abastecimento de combustíveis em veículos por postos credenciados, conforme termo de referência do anexo IX. Renovação do prazo e valor, 12 meses, R$ 4.609.752,00, 02.16.01 - 3.3.90.39.00, 18-12-2025; Cad. 801/25, CP 002/22, PF 4.089/22, Romarello Terraplenagem e Construções Ltda, Quinto Aditamento ao Contrato para a "execução de pavimentação asfáltica e serviços complementares, com fornecimento de materiais, mão de obra e equipamentos". Acréscimo de valor (R$ 563.643,03) e Supressão (R$ 18.300,24). Prorrogação dos prazos, 150 dias, 02.16.01-3.3.90.39.00, 19-12-2025; Cad. 802/25, Ch. Pública 005/24, PF 3.307/24, Terradan Terraplenagem de Artur Nogueira Ltda, Quarto aditamento ao contrato para execução das obras de pavimentação asfáltica e serviços complementares, com fornecimento de materiais, mão de obra e equipamentos, conforme Planilhas de orçamento, memorial descritivo e projetos. Prorrogação dos prazos, 120 dias, 19-12-2025; SECRETARIA DE SAÚDE: Cad. 594/25, PE 083/24, PF 6.745/24, Lilian Cristina Rodrigues Rosa Chaves, Primeiro Aditamento à Ata de Registro de Preços para aquisição de medicamentos para atendimentos de mandados judiciais. Prorrogação do prazo e renovação dos quantitativos, 12 meses, 12-12-2025; Cad. 595/25, PE 083/24, PF 6.745/24, A.D. Daminelli Ltda, Primeiro Aditamento à Ata de Registro de Preços para aquisição de medicamentos para atendimentos de mandados judiciais. Prorrogação do prazo e renovação dos quantitativos, 12 meses, 12-12-2025; Cad. 596/25, PE 083/24, PF 6.745/24, C.M. Hospitalar S/A, Primeiro Aditamento à Ata de Registro de Preços para aquisição de medicamentos para atendimentos de mandados judiciais. Prorrogação do prazo e renovação dos quantitativos, 12 meses, 12-12-2025; Cad. 597/25, PE 083/24, PF 6.745/24, Gabriel da Gama Galache, Primeiro Aditamento à Ata de Registro de Preços para aquisição de medicamentos para atendimentos de mandados judiciais. Prorrogação do prazo e renovação dos quantitativos, 12 meses, 12-12-2025; Cad. 598/25, PE 083/24, PF 6.745/24, W.A. Comércio de Medicamentos Ltda, Primeiro Aditamento à Ata de Registro de Preços para aquisição de medicamentos para atendimentos de mandados judiciais. Prorrogação do prazo e renovação dos quantitativos, 12 meses, 12-12-2025; Cad. 599/25, PE 083/24, PF 6.745/24, Josiane Cristina Fusco Carraro -Epp, Primeiro Aditamento à Ata de Registro de Preços para aquisição de medicamentos para atendimentos de mandados judiciais. Prorrogação do prazo e renovação dos quantitativos, 12 meses, 12-12-2025; Cad. 600/25, PE 083/24, PF 6.745/24, Xismed Distribuidora Ltda, Primeiro Aditamento à Ata de Registro de Preços para aquisição de medicamentos para atendimentos de mandados judiciais. Prorrogação do prazo e renovação dos quantitativos, 12 meses, 12-12-2025; Cad. 601/25, PE 111/25, PF 6.020/25, PMI Brasil Importadora e Exportadora de Produtos Para Saúde Ltda, Ata de Registro de Preços para aquisição de materiais de enfermagem diversos para atendimento da demanda das unidades de saúde, 12 meses, 15-12-2025; Cad. 602/25, PE 111/25, PF 6.020/25, Arlimed Distribuidora Hospitalar Ltda, Ata de Registro de Preços para aquisição de materiais de enfermagem diversos para atendimento da demanda das unidades de saúde, 12 meses, 15-12-2025; Cad. 603/25, PE 111/25, PF 6.020/25, Tetra Farm Indústria e Comércio de Material Hospitalar Ltda, Ata de Registro de Preços para aquisição de materiais de enfermagem diversos para atendimento da demanda das unidades de saúde, 12 meses, 15-12-2025; Cad. 604/25, PE 111/25, PF 6.020/25, RMP Distribuidora Ltda, Ata de Registro de Preços para aquisição de materiais de enfermagem diversos para atendimento da demanda das unidades de saúde, 12 meses, 15-12-2025; Cad. 605/25, PE 111/25, PF 6.020/25, Medicina Segura Distribuição e Promoção de Vendas Ltda, Ata de Registro de Preços para aquisição de materiais de enfermagem diversos para atendimento da demanda das unidades de saúde, 12 meses, 15-12-2025; Cad. 606/25, PE 111/25, PF 6.020/25, Soma/SP Produtos Hospitalares Ltda, Ata de Registro de Preços para aquisição de materiais de enfermagem diversos para atendimento da demanda das unidades de saúde, 12 meses, 15-12-2025; Cad. 607/25, PE 111/25, PF 6.020/25, Millenium Comércio Serviço Ltda, Ata de Registro de Preços para aquisição de materiais de enfermagem diversos para atendimento da demanda das unidades de saúde, 12 meses, 15-12-2025; Cad. 608/25, PE 107/25, PF 3.632/25, Inova Care Produtos Para Saúde Ltda, Ata de Registro de Preços para aquisição de insumos para atendimento de mandados judiciais, 12 meses, 15-12-2025; Cad. 609/25, PE 107/25, PF 3.632/25, Matheus Comércio Atacadista Ltda, Ata de Registro de Preços para aquisição de insumos para atendimento de mandados judiciais, 12 meses, 15-12-2025; Cad. 610/25, PE 107/25, PF 3.632/25, Gemeli Medical Ltda, Ata de Registro de Preços para aquisição de insumos para atendimento de mandados judiciais, 12 meses, 15-12-2025; Cad. 611/25, PE 107/25, PF 3.632/25, Abbott Laboratórios do Brasil Ltda, Ata de Registro de Preços para aquisição de insumos para atendimento de mandados judiciais, 12 meses, 15-12-2025; Cad. 612/25, PE 107/25, PF 3.632/25, G2 Comércio e Serviços Ltda, Ata de Registro de Preços para aquisição de insumos para atendimento de mandados judiciais, 12 meses, 15-12-2025; Cad. 613/25, PE 107/25, PF 3.632/25, DMS Medicamentos e Material Médico Hospitalar Ltda, Ata de Registro de Preços para aquisição de insumos para atendimento de mandados judiciais, 12 meses, 15-12-2025; Cad. 614/25, PE 107/25, PF 3.632/25, V.R. Valadares Suprimentos Ltda, Ata de Registro de Preços para aquisição de insumos para atendimento de mandados judiciais, 12 meses, 15-12-2025; Cad. 615/25, PE 107/25, PF 3.632/25, Cirúrgica Califórnia Ltda, Ata de Registro de Preços para aquisição de insumos para atendimento de mandados judiciais, 12 meses, 15-12-2025; Cad. 616/25, PE 107/25, PF 3.632/25, Campsupply Hospitalar Ltda, Ata de Registro de Preços para aquisição de insumos para atendimento de mandados judiciais, 12 meses, 15-12-2025; Cad. 617/25, PE 107/25, PF 3.632/25, Special Med Comercial Hospitalar Ltda, Ata de Registro de Preços para aquisição de insumos para atendimento de mandados judiciais, 12 meses, 15-12-2025; Cad. 770/25, PF 9.223/25, Associação Ecumênica de Promoção Humana, Inclusão e Valorização de Americana - AEPHIVA, Termo de Fomento para a execução da atividade/projeto AEPHIVA - Casa de Apoio, 12 meses, R$ 32.315,52, 05.300.0543 / 05.300.0527, 12-12-2025; Cad. 771/25, Disp. Lic. 957/25, PF 12.006/25, Associação Americanense de Saúde, Contrato para a contratação de serviço médico especializado para realização de procedimento cirúrgico, conforme determinação judicial, 180 dias, R$ 70.578,00, 02.14.01 - 3.3.90.39.00, 15-12-2025; Cad. 773/25, CRED 004/25, PF 3.631/25, Residencial Vita Sênior Eireli, Contrato para credenciamento da Credenciada para a prestação de serviço de acolhimento de idosos, do sexo feminino ou masculino, Grau III de dependência, 12 meses, R$ 720.000,00,

02.14.01.33.90.39.00, 16-12-2025; Cad. 778/25, PP 052/23, PF 10.390/23, Matheus Duarte Viel, Terceiro Aditamento ao Contrato para prestação de serviços de desinsetização e desratização nas unidades da secretaria de saúde. Renovação do prazo e reprogramação do objeto Acréscimo (R$ 1.666,72), 12 meses, R$ 31.667,68, 02.1601/ 02.14.01 - 3.3.90.39, 18-12-2025; Cad. 781/25, CP 003/25, PF 10.730/24, Home Construções e Serviços Ltda, Primeiro Aditamento ao Contrato para a execução de obras de reforma de salas do Hospital Municipal Dr. Waldemar Tebaldi para instalação do Programa Mamãe Nenê, no município de Americana, com fornecimento de materiais, mão-de-obra e equipamentos. Retificação ao regime de execução da obra, 18-12-2025; Cad. 782/25, PF 206/24, Unidade de Apoio Aos Portadores de Câncer - UNIAP, Segundo aditamento ao termo de parceria para definir a inserção da entidade no SUS de forma não onerosa, por meio de ações de promoção à saúde, em especial para regulamentar a execução de ações e serviços de promoção à saúde. Prorrogação do prazo, 12 meses, 18-12-2025; Cad. 783/25, PE 139/23, PF 10.339/23, Radiologia Sidney de Souza Almeida Ltda, Segundo Aditamento ao Contrato para a prestação de serviços de procedimentos com finalidade diagnóstica de exames de biópsias de mama percutânea por estereotaxia. Renovação do prazo e valor, 12 meses, R$ 65.869,00, 002.014.0040-3.3.90.39.00/50, 18-12-2025;

Eu, Maria da Graça Fontana Cuaino, matrícula 2496, elaborei e conferi o presente edital. Eu, José Eduardo da Cruz Rodrigues Flores, Secretário Adjunto de Administração, autorizei a publicação oficial.

Americana, 19 de Dezembro de 2025.

DECRETO Nº 13.889, DE19 DE DEZEMBRO DE 2025.

"Aprova o plano de desmembramento de gleba de propriedade de Politano Patrimonial Ltda., na forma que específica, e dá outras providências."

Francisco Antonio Sardelli, Prefeito Municipal de Americana, no uso das atribuições que lhe são conferidas por lei;

Considerando o disposto no art. 62, inciso V, da Lei Orgânica do Município de Americana;

Considerando o disposto nos artigos 52 e seguintes, da Lei Municipal n° 6.994, de 11 de setembro de 2025, e;

Considerando, finalmente, os elementos que integram o processo administrativo digital PMA - Análise de Projeto n° 1.289/2024,

D E C R E T A :

Art. 1º Fica aprovado o plano de desmembramento de gleba com 1.979,56m² (um mil, novecentos e setenta e nove metros quadrados e cinquenta e seis centímetros quadrados), situado na Rua Orozimbo Machado, gleba 01, Bairro São Vito, nesta cidade, cadastrada sob o nº 13.0065.0097.0000, objeto da matrícula nº 107.394, do Cartório de Registro de Imóveis local, de propriedade de Politano Patrimonial Ltda., conforme planta aprovada nº 106.959, de 08 de dezembro de 2025, que passa a ser constituída por:

I - Lote 01A, com 324,19m² (trezentos e vinte e quatro metros quadrados e dezenove centímetros quadrados);
II - Lote 01B, com 1.655,37m² (um mil, seiscentos e cinquenta e cinco metros quadrados e trinta e sete centímetros quadrados).

Art. 2º Na execução do plano de desmembramento, deverá ser observada a legislação pertinente, em especial a Lei Municipal n° 6.994, de 11 de setembro de 2025.

Art. 3º Este Decreto entra em vigor na data de sua publicação, revogadas as disposições em contrário.

Prefeitura Municipal de Americana, aos 18 de dezembro de 2025.

Publicado na mesma data na Secretaria de Administração

FRANCISCO ANTONIO SARDELLI
PREFEITO MUNICIPAL

JOSÉ EDUARDO DA CRUZ RODRIGUES FLORES
SECRETÁRIO ADJUNTO DE ADMINISTRAÇÃO

MAURICIO MARZOCHI
SECRETÁRIO MUNICIPAL DE NEGÓCIOS JURÍDICOS

LEI Nº 7.044, DE 19 DE DEZEMBRO DE 2025.

Autor do Projeto de Lei C. M. nº 185/2025 - Poder Executivo - Francisco Antonio Sardelli.

"Dispõe sobre a desafetação e doação de imóvel que especifica."

Francisco Antonio Sardelli, Prefeito Municipal de Americana, no uso das atribuições que lhe são conferidas por lei, faz saber que a Câmara Municipal aprovou e ele sanciona e promulga a seguinte lei:

Art. 1º Fica transferido da categoria de "Sistema de Lazer III" para a categoria de "Bem de Uso Institucional", o imóvel a seguir descrito:

Proprietário: Município de Americana
Local: Rua Francisca Coral Chiquinho - Jardim Terramérica II - Americana/SP
Cadastro: 27.0080.0190.0000

Descrição: "Inicia-se num ponto localizado no alinhamento da Rua Francisca Coral Chiquinho e segue em reta pelo referido alinhamento numa distância de 86,28m (oitenta e seis metros e vinte e oito centímetros); deste segue em curva à esquerda na confluência da Rua Francisca Coral Chiquinho com Rua Pedro Nicoletti numa distância de 16,79m (dezesseis metros e setenta e nove centímetros); deste segue em reta pelo alinhamento da Rua Pedro Nicoletti numa distância de 99,75m (noventa e nove metros e setenta e cinco centímetros); deste segue em curva à esquerda na confluência da Rua Pedro Nicoletti com Rua Laudelino Basseto numa distância de 14,14m (quatorze metros e quatorze centímetros); deste segue em reta pelo alinhamento da Rua Laudelino Basseto numa distância de 85,22m (oitenta e cinco metros e vinte e dois centímetros); deste deflete à esquerda e segue em reta divisando com remanescente do Sistema de Lazer III numa distância de 92,56m (noventa e dois metros e cinquenta e seis centímetros) até o ponto inicial, perfazendo uma área superficial de 10.003,75m² (dez mil, três metros quadrados e setenta e cinco centímetros quadrados)."

Art. 2º Fica o Poder Executivo autorizado a doar à Câmara Municipal de Americana, a área descrita no artigo anterior, para o fim específico de construção, implantação e funcionamento da sede do Poder Legislativo Municipal.

Art. 3º Caberá ao Poder Executivo providenciar a abertura da matrícula específica da mencionada área pública, outorgando, posteriormente, à Câmara Municipal de Americana a competente escritura pública de doação.

Art. 4º As obras de construção deverão ser iniciadas no prazo de 24 (vinte e quatro) meses, prorrogável por idêntico período, contados da data de lavratura da escritura de doação sob pena de revogação da referida doação e consequente reversão do imóvel ao Poder Público Municipal.

Art. 5º As despesas decorrentes da transferência do imóvel serão de responsabilidade do doador e correrão por conta de dotação própria constante do orçamento.

Art. 6º Esta Lei entra em vigor na data de sua publicação.

Prefeitura Municipal de Americana, aos 19 de dezembro de 2025.

Ref. Prot. Digital PMA nº 143.013/2025.

Publicado na mesma data na Secretaria de Administração

FRANCISCO ANTONIO SARDELLI
PREFEITO MUNICIPAL

JOSÉ EDUARDO DA CRUZ RODRIGUES FLORES
SECRETÁRIO ADJUNTO DE ADMINISTRAÇÃO

MAURICIO MARZOCHI
SECRETÁRIO MUNICIPAL DE NEGÓCIOS JURÍDICOS

LICITAÇÃO

EXTRATO DE DISPENSA DE LICITAÇÃO E INEXIGIBILIDADE
RELAÇÃO DE DISPENSA DE LICITAÇÃO E INEXIGIBILIDADE nos quais figuram como contratante a Prefeitura Municipal de Americana, que contém o número do processo administrativo, o nome ou a razão social do contratado, o objeto, o valor e a Secretaria requisitante.
DISPENSA Nº 967/2025, PROCESSO Nº 3141/2023 - OBJETO PAGAMENTO DE FRANQUIA DE SEGURO VEÍCULO, PLACA: SUL-9J64 - SEC. OBRAS CONTRATO: ENTREGA ÚNICA - VALOR TOTAL R$ 561,00 - FORNECEDOR GERMANICA LOCADORA DE VEICULOS LIMITADA; **DISPENSA Nº 969/2025,** PROCESSO Nº 13.273/2025 - OBJETO SERVIÇO DE MANUTENÇÃO E REVISÃO EM MÁQUINA DE LAVAR ROUPA - EMEI ARAÇARI CONTRATO: ENTREGA ÚNICA - VALOR TOTAL R$ 950,00 - FORNECEDOR LUIZ CLÁUDIO MIANO-ME;
DISPENSA Nº 970/2025, PROCESSO Nº 11.914/2025 - OBJETO CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DE SERVIÇOS DE ENGENHARIA - SECRETARIA DE ADMINISTRAÇÃO CONTRATO: Á REALIZAR - VALOR TOTAL R$ 18.850,00 - FORNECEDOR RM INSTALAÇÕES INDUSTRIAIS LTDA-EPP; **DISPENSA Nº 971/2025,** PROCESSO Nº 13.454/2025 - OBJETO CONTRATAÇÃO DE 12 (DOZE) MESES DA LICENÇA TRELLO PREMIUM, PLATAFORMA ONLINE DE GESTÃO DE PROJETOS E COLABORAÇÃO - SEC. DE COMUNICAÇÃO E TECNOLOGIA DA INFORMAÇÃO CONTRATO: Á REALIZAR - VALOR TOTAL R$ 11.400,00 - FORNECEDOR L3 INFORMÁTICA LTDA; **DISPENSA Nº 973/2025,** PROCESSO Nº 11.865/2025 - OBJETO SERVIÇO DE MANUTENÇÃO CORRETIVA COM TROCA DE PEÇAS, PLACA:SWH-2C32, SEC. SAÚDE CONTRATO: ENTREGA ÚNICA - VALOR TOTAL R$ 8.748,00 - FORNECEDOR PEPE & LUIZ MECANICA LTDA; **DISPENSA Nº 974/2025**, PROCESSO Nº 14.260/2025 - OBJETO SERVIÇO DE CHAVEIRO PARA CONSERTO DE FECHADURAS NA SEC. FAZENDA CONTRATO: ENTREGA ÚNICA - VALOR TOTAL R$ 302,00 - FORNECEDOR WD CHAVEIRO LTDA; **DISPENSA Nº 975/2025,** PROCESSO Nº 14.259/2025 - OBJETO SERVIÇO DE PASSAGEM AÉREA PARA SERVIDORES DA UNIDADE DE SUPRIMENTOS - SECRETARIA DE ADMINISTRAÇÃO CONTRATO: ENTREGA ÚNICA - VALOR TOTAL R$ 5.735,76 - FORNECEDOR FAE VIAGENS E TURISMO LTDA ME; **DISPENSA Nº 977/2025,** PROCESSO Nº 9659/2025 - OBJETO CONTRATAÇÃO DE INSTITUIÇÃO ESPECIALIZADA PARA FORMAÇÃO DOS AGENTES CULTURAIS E SERVIDORES PÚBLICOS EM ACESSIBILIDADE NA ELABORAÇÃO DE PROJETOS CULTURAIS - SEC. DE CULTURA CONTRATO: Á REALIZAR - VALOR TOTAL R$ 15.000,00 - FORNECEDOR SENAC - SERVICO NACIONAL DE APRENDIZAGEM; **DISPENSA Nº 978/2025,** PROCESSO Nº 14.016/2025 - OBJETO AQUISIÇÃO DE MEDICAMENTO LEUPRORRELINA ACETATO PARA SUPRIR DEMANDA DA ATENÇÃO BÁSICA - SECRETARIA DE SAÚDE CONTRATO: ENTREGA ÚNICA - VALOR TOTAL R$ 1.316,70 - FORNECEDOR ONCOVIT DISTRIBUIDORA DE MEDICAMENTOS LTDA; **DISPENSA Nº 979/2025,** PROCESSO Nº 12.412/2025 - OBJETO AQUISIÇÃO DE PEÇAS PARA MANUTENÇÃO DO VEÍCULO MODELO MASTER MINIBUSL3 - PLACA: SWS-1B22 - SECRETARIA DE SAÚDE CONTRATO: ENTREGA ÚNICA - VALOR TOTAL R$ 890,00 - FORNECEDOR LAFER AUTO PEÇAS LTDA-ME; **DISPENSA Nº 980/2025,** PROCESSO Nº 12.239/2025 - OBJETO AQUISIÇÃO DE MEDICAMENTOS PARA ATENDIMENTO DE MANDADOS JUDICIAIS CONFORME TERMO DE REFERENCIA - SEC. SAUDE CONTRATO: ENTREGA ÚNICA - VALOR TOTAL R$ 2.869,20 - FORNECEDOR DROGA PIRES DE AMERICANA LTDA-EPP, VALOR TOTAL R$ 338,40 - FORNECEDOR H.H. CAVALARO LTDA; **INEXIGIBILIDADENº 46/2025,** PROCESSO Nº 13.603/2025 - OBJETO PALESTRA MOTIVOCIONAL PARA ATLETAS DO JUDÔ - SEC. ESPORTES CONTRATO: A REALIZAR - VALOR TOTAL R$ 30000,00 - FORNECEDOR FEDERACAO NACIONAL DOS CLUBES ESPORTIVOS - FENACLUBES.

EXTINÇÃO DE AUTORIZAÇÃO DE FORNECIMENTO
DISPENSA N.º 728/2025
Processo n.º 8.528/2025.
OBJETO: "AQUISIÇÃO EMERGENCIAL DE MATERIAIS DE LIMPEZA - SEC. SAÚDE".
A Prefeitura Municipal de Americana torna pública a extinção consensual das autorizações de fornecimento 4051/2025, 4055/2025 e 4113/2025 da empresa **FKK DISTRIBUIDORA LTDA** conforme decisão do Secretário de Saúde, em acolhimento ao parecer jurídico da Secretaria de Negócios Jurídicos, fundamentada no artigo 138, II da Lei 14.133/2021. Eu, Cesar Ricardo Montanari, matrícula n.º 14.218, conferi o presente. Eu, José Eduardo da Cruz Rodrigues Flores, Secretário Adjunto de Administração, autorizei a publicação oficial. Americana, 19 de Dezembro de 2025.

SECRETARIA DE OBRAS E SERVIÇOS URBANOS

UNIDADE DE TRANSPORTES E SISTEMA VIÁRIO

SETOR DE MULTAS

Fica o interessado cientificado do julgamento proferido CETRAN - Conselho Estadual de trânsito - 2º instância.

PROCEDENTE

Protocolos:

72.626/2025 Placa FUS5J94

Maiores informações, entrar em contato com esta Secretaria, no Setor de Multas na Av. Bandeirantes,600 - bairro Lot. Industrial.

Americana, 19 de dezembro de 2025

ENGº MARCELO MAIA GIONGO
AUTORIDADE DE TRÂNSITO

GUARDA MUNICIPAL DE AMERICANA (GAMA)

UNIDADE DE CORREGEDORIA

PORTARIA N° 07, DE 19 DE DEZEMBRO DE 2025.
"Decisão em Processo Administrativo Disciplinar"

RODRIGO DIAS, CORREGEDOR GERAL da GUARDA MUNICIPAL DE AMERICANA, no uso das atribuições que lhe são conferidas por lei e pela Portaria nº 87 de 23 de maio de 2024.

Considerando o Art. 86 § 2º da Lei Municipal 6.874/2024.

R E S O L V E:

I-TORNAR PÚBLICA a Decisão em Processo Administrativo Disciplinar nº **0000132-019.2025.0102**,relacionado ao empregado público de matrícula nº **1341**, com fundamento no artigo 95, incisos VI (incontinência de conduta ou mau procedimento) e VIII (ofensa física em serviço ou em razão dele, contra servidor ou particular), ambos da lei municipal nº 6.874, de 17 de maio de 2024, C/C Artigo 177, incisos VI e VIII, da Lei Municipal nº 5.110/2010, de 23 de novembro de 2010, que resultou na aplicação da sanção disciplinar de **DEMISSÃO POR JUSTA CAUSA**.
.
II- Esta portaria entra em vigor na data de sua publicação.

Americana, 19 de dezembro de 2025

RODRIGO DIAS
CORREGEDOR GERAL

ERRATA
PORTARIA N° 06, DE 15 DE DEZEMBRO DE 2025

Onde se Lê:

I- Considerando o Decreto Municipal 13.868 de 27 de novembro de 2025 e o Art. 152 § 1º da Lei Municipal 6.874/2024, ficam suspensos os prazos processuais, as audiências e as sessões de julgamento **entre o período de 22 de dezembro de 2024 a 05 de janeiro de 2025.**

Leia se:

I- Considerando o Decreto Municipal 13.868 de 27 de novembro de 2025 e o Art. 152 § 1º da Lei Municipal 6.874/2024, ficam suspensos os prazos processuais, as audiências e as sessões de julgamento entre o período de **22 de dezembro de 2025 a 02 de janeiro de 2026.**

Americana, 19 de dezembro de 2025

RODRIGO DIAS
CORREGEDOR GERAL

DEPARTAMENTO DE ÁGUA E ESGOTO

EDITAL DE ABERTURA DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 33/25
PROCESSO ADMINISTRATIVO Nº 859//2025
OBJETO: Contratação de empresa de engenharia para a prestação de serviços de pesquisa, localização e correção de vazamentos não aparentes no sistema de abastecimento de água do município de Americana, com fornecimento de mão de obra, materiais, equipamentos e todos os serviços correlatos, nos termos abaixo, conforme condições, quantidades e exigências estabelecidas no termo de referência.
Abertura das Propostas: 20 de janeiro de 2026, **a partir das 08h30min**
Inicio da Sessão de disputa de Preços: 20 de janeiro de 2026, a partir das 08h35min
Endereço Eletrônico: www.novobbmnet.com.br
Fones: (19) 3471 2904 / 2948
Email: licitacao@daeamericana.sp.gov.br
O Edital está disponível através do site: www.daeamericana.sp.gov.br - link: Editais e Licitações: Pregões Eletrônicos.

Americana, 19 de dezembro de 2025

LÍVIA GUIMARÃES ZERAIK CARDOSO
SUPERINTENDENTE ADJUNTA DE GESTÃO

SECRETARIA DE FAZENDA

UNIDADE DE TRIBUTAÇÃO

EDITAL Nº 115 / 2025
Edital de Análise Definitiva dos Pedidos de Isenção de IPTU do Exercício de 2025.

Edital de Análise Definitiva dos Pedidos de Isenção de IPTU do Exercício de 2025. A Secretaria de Fazenda, por meio da Unidade de Julgamento de Processos Administrativos, FAZ SABER a todos os interessados, que, com fundamento no art. 35 da Lei nº 4.930/2009, com a redação dada pela Lei nº 6.573/2021; na Lei nº 5.047/2010, com a redação dada pela Lei nº 6.165/2018 e no Decreto nº 12.823/2021, **os pedidos relacionados no Anexo I foram INDEFERIDOS em razão do descumprimento dos requisitos para a concessão da isenção do IPTU lançado no exercício de 2025**. Os contribuintes que formalizaram os pedidos de isenção devem acompanhar os resultados na plataforma digital disponibilizada no site da Prefeitura de Americana (https://americana.1doc.com.br), conforme previsto no inciso VII do art. 5º do Decreto nº 12.873/2021; ou pelo telefone (19) 3475-9049. E para que produza efeitos jurídicos e legais, e não possa ser alegada ignorância, expediu-se o presente Edital, devidamente publicado na forma da Lei.

Prefeitura de Americana, 18 de dezembro de 2025.

ANDERSON NATEL FERREIRA
Diretor da Unidade de Julgamento de Processos Administrativos

Edital nº 115/2025 • Isenção IPTU • INDEFERIDOS Análise Definitiva

ANEXO I

ANÁLISE Definitiva DOS PROCESSOS DE ISENÇÃO DE IPTU/2025		
RESULTADOS: INDEFERIDOS		
Nº PROTOCOLO	Nº CADASTRO	RESULTADO
PD00499/2025	26012801030000	Indeferido
PD00509/2025	15065003800134	Indeferido
PD00672/2025	19003001570000	Indeferido
PD00767/2025	07013101980000	Indeferido
PD00774/2025	19021001430000	Indeferido
PD00802/2025	36013702180000	Indeferido
PD00820/2025	16058000510408	Indeferido
PD00827/2025	11008701770000	Indeferido
PD00916/2025	22004404730001	Indeferido
PD01087/2025	03003401360000	Indeferido
PD01171/2025	19026101970000	Indeferido
PD01209/2025	19020801030000	Indeferido
PD01250/2025	10003101830000	Indeferido
PD01272/2025	27060001100538	Indeferido
PD01312/2025	22001100810000	Indeferido
PD01430/2025	17004100230000	Indeferido
PD01553/2025	19027204700134	Indeferido
PD01598/2025	23009200800010	Indeferido
PD01660/2025	13006302630000	Indeferido
PD01871/2025	07006809590598	Indeferido
PD02055/2025	23005803700002	Indeferido
PD02145/2025	04011401750077	Indeferido
PD02265/2025	19028400190000	Indeferido
PD02354/2025	15010402440000	Indeferido
PD02556/2025	15002202360000	Indeferido
PD02595/2025	36010300100000	Indeferido
PD02660/2025	26008801950000	Indeferido
PD02701/2025	15001700680000	Indeferido
PD02732/2025	11096000200843	Indeferido
PD02738/2025	21004100760035	Indeferido
PD02888/2025	36001400950000	Indeferido
PD02967/2025	26014101910000	Indeferido
PD02977/2025	35055000820608	Indeferido
PD03194/2025	15008301460000	Indeferido
PD03280/2025	16009202200000	Indeferido
PD03345/2025	30003502560000	Indeferido
PD03351/2025	35004400890000	Indeferido
PD03362/2025	14001200420000	Indeferido
PD03382/2025	19007900250000	Indeferido
PD03765/2025	19034200310000	Indeferido
PD03783/2025	11011900820000	Indeferido
PD03805/2025	36020902900000	Indeferido
PD03868/2025	16008401270000	Indeferido
PD03892/2025	36014502590000	Indeferido
PD03996/2025	26000101220000	Indeferido
PD04018/2025	19023600820000	Indeferido

Edital nº 115/2025 • Isenção IPTU • INDEFERIDOS Análise Definitiva

PD04030/2025	35001202250055	Indeferido
PD04039/2025	19022101800000	Indeferido
PD04045/2025	23021002330083	Indeferido
PD04052/2025	19001704020000	Indeferido
PD04105/2025	04011401750052	Indeferido
PD04162/2025	07004800350000	Indeferido
PD04179/2025	16005402000000	Indeferido
PD04202/2025	16058000510230	Indeferido
PD04216/2025	11102500910192	Indeferido
PD04239/2025	19014102750000	Indeferido
PD04321/2025	16004403520000	Indeferido
PD04401/2025	23006201850000	Indeferido
PD04407/2025	36019801860000	Indeferido
PD04511/2025	05004002630000	Indeferido
PD04619/2025	07004203780001	Indeferido
PD04744/2025	16004000700000	Indeferido
PD04748/2025	11009700590000	Indeferido
PD04766/2025	19100001300041	Indeferido
PD04767/2025	30004003660000	Indeferido
PD04808/2025	19022003370000	Indeferido
PD04942/2025	19017601060000	Indeferido
PD05012/2025	30003101560000	Indeferido
PD05020/2025	15008703680000	Indeferido
PD05037/2025	08007500350000	Indeferido
PD05041/2025	26073000280056	Indeferido
PD05067/2025	26012402540000	Indeferido
PD05074/2025	20011601750024	Indeferido
PD05144/2025	23002703030003	Indeferido
PD05211/2025	19025803040000	Indeferido
PD05302/2025	30003703280000	Indeferido
PD05320/2025	26001705400000	Indeferido
PD05321/2025	08007501720000	Indeferido
PD05338/2025	30003302880000	Indeferido
PD05403/2025	36024604230000	Indeferido
PD05410/2025	15007801150000	Indeferido
PD05473/2025	19026904600000	Indeferido
PD05558/2025	14012303090000	Indeferido
PD05618/2025	36024500250000	Indeferido
PD05747/2025	22004401920000	Indeferido
PD05796/2025	36004301090000	Indeferido
PD05903/2025	11096000200407	Indeferido
PD05940/2025	11015602830000	Indeferido
PD06133/2025	19027803240000	Indeferido
PD06165/2025	04003001450000	Indeferido
PD06188/2025	19020202630000	Indeferido
PD06299/2025	36013602590000	Indeferido
PD06358/2025	16001403170000	Indeferido
PD06387/2025	11005200290000	Indeferido
PD06421/2025	23010002010000	Indeferido
PD06453/2025	15015701030000	Indeferido
PD06555/2025	36019500560000	Indeferido
PD06632/2025	07004202580000	Indeferido

Edital nº 115/2025 • Isenção IPTU • INDEFERIDOS Análise Definitiva

PD06837/2025	19100001400119	Indeferido
PD06875/2025	24078001100031	Indeferido
PD06886/2025	19027800990000	Indeferido
PD06895/2025	23000302980000	Indeferido
PD06902/2025	19017201630000	Indeferido
PD07050/2025	30003403520000	Indeferido
PD07061/2025	19016803550000	Indeferido
PD07098/2025	26073000300415	Indeferido
PD07105/2025	16009600760000	Indeferido
PD07197/2025	16058000510131	Indeferido
PD07280/2025	19024504150000	Indeferido
PD07299/2025	23010201510000	Indeferido
PD07342/2025	27055002000519	Indeferido
PD07374/2025	36002304030000	Indeferido
PD07496/2025	23002302550000	Indeferido
PD07549/2025	10002902130014	Indeferido
PD07672/2025	15002201590000	Indeferido
PD07705/2025	23006601920000	Indeferido
PD07736/2025	16001000410000	Indeferido
PD07755/2025	36024000710000	Indeferido
PD07795/2025	19009800740000	Indeferido
PD07801/2025	23019401170000	Indeferido
PD07805/2025	15014002140000	Indeferido
PD07931/2025	24004800770000	Indeferido
PD07965/2025	19030604200001	Indeferido
PD07986/2025	36023201740000	Indeferido
PD08065/2025	26073000280306	Indeferido
PD08139/2025	14015503570000	Indeferido
PD08270/2025	20004605040000	Indeferido
PD08341/2025	24005903500000	Indeferido
PD08365/2025	35055000600235	Indeferido
PD08410/2025	19020400900000	Indeferido
PD08475/2025	26011102210000	Indeferido
PD08500/2025	24078001300583	Indeferido
PD08516/2025	25001404340000	Indeferido
PD08564/2025	11005302920000	Indeferido
PD08769/2025	19005100670000	Indeferido
PD08803/2025	24005403390000	Indeferido
PD08858/2025	19032301530000	Indeferido
PD08908/2025	04002803300000	Indeferido
PD08981/2025	19018100490000	Indeferido
PD09113/2025	15000801290000	Indeferido
PD09663/2025	08006402180000	Indeferido
PD09664/2025	26073000280342	Indeferido
PD09776/2025	21007204150000	Indeferido
PD09837/2025	30005201840000	Indeferido
PD10317/2025	08005601840012	Indeferido
PD10386/2025	04005800960001	Indeferido
PD10426/2025	23020700930000	Indeferido
PD10458/2025	03006701530000	Indeferido
PD10514/2025	19030801540000	Indeferido
PD10538/2025	27004400860000	Indeferido

Edital nº 115/2025 • Isenção IPTU • INDEFERIDOS Análise Definitiva

PD10617/2025	08001001900000	Indeferido
PD10637/2025	15015200840000	Indeferido
PD10640/2025	27002402420114	Indeferido
PD10934/2025	36021401270000	Indeferido
PD11121/2025	23013302000000	Indeferido
PD11130/2025	19008900430000	Indeferido
PD11184/2025	19028300940000	Indeferido
PD11272/2025	26073000300317	Indeferido
PD11279/2025	19031101180000	Indeferido
PD11532/2025	11102500910052	Indeferido
PD11569/2025	08000301800000	Indeferido
PD11603/2025	19029502320000	Indeferido
PD11773/2025	19015202770000	Indeferido
PD12376/2025	09001400250000	Indeferido
PD13788/2025	21006100610000	Indeferido
PD13889/2025	18001806150051	Indeferido
PD13957/2025	12000300710000	Indeferido
PD14133/2025	17005700850000	Indeferido
PD14573/2025	17006803530000	Indeferido
PD14577/2025	07005602590000	Indeferido
PD14719/2025	04002001340000	Indeferido
PD15288/2025	19023800900000	Indeferido
PD15938/2025	26073000300181	Indeferido
PD16141/2025	19017302530000	Indeferido
PD16170/2025	15010202380000	Indeferido
PD16435/2025	16007104310000	Indeferido
PD16639/2025	24003904150000	Indeferido
PD16674/2025	35011401710000	Indeferido
PD16797/2025	15065004100679	Indeferido
PD16812/2025	14012202210000	Indeferido
PD16974/2025	35005800970000	Indeferido
PD17348/2025	19017301090000	Indeferido
PD17359/2025	24078001300195	Indeferido
PD17551/2025	05002202820002	Indeferido
PD17862/2025	26073000280257	Indeferido
PD17874/2025	30003202820000	Indeferido
PD18100/2025	12001201700000	Indeferido
PD18114/2025	06000502890048	Indeferido
PD18266/2025	04010903330000	Indeferido
PD18362/2025	26011602660001	Indeferido
PD18391/2025	15008700990000	Indeferido
PD18471/2025	24006800840000	Indeferido
PD18481/2025	19100001200209	Indeferido
PD18839/2025	19025700670000	Indeferido
PD19122/2025	15001201600001	Indeferido
PD19204/2025	17007403400000	Indeferido
PD19355/2025	19026802900000	Indeferido
PD19490/2025	15014604270000	Indeferido
PD19554/2025	15065003700124	Indeferido
PD19643/2025	19027700990000	Indeferido
PD19992/2025	22012102380019	Indeferido
PD20008/2025	26073000280194	Indeferido

Edital nº 115/2025 • Isenção IPTU • INDEFERIDOS Análise Definitiva

PD20040/2025	24000901720000	Indeferido
PD21048/2025	36023403300000	Indeferido
PD21199/2025	36024200500000	Indeferido
PD22237/2025	16001900810000	Indeferido
PD22580/2025	19100001400256	Indeferido
PD22659/2025	26073000280216	Indeferido
PD23082/2025	19022603500000	Indeferido
PD23195/2025	11007301480000	Indeferido
PD23338/2025	19070000200118	Indeferido
PD23369/2025	11011901060000	Indeferido
PD23433/2025	24003904000000	Indeferido
PD23641/2025	36006000380002	Indeferido
PD24245/2025	23000502650000	Indeferido
PD24313/2025	14012403530000	Indeferido
PD24829/2025	20007201230074	Indeferido
PD25040/2025	14005800900000	Indeferido
PD25126/2025	19020501800000	Indeferido
PD25309/2025	18062000500076	Indeferido
PD25355/2025	36024202370000	Indeferido
PD25396/2025	19025900370000	Indeferido
PD25579/2025	16006102670000	Indeferido
PD25643/2025	19026202800000	Indeferido
PD25703/2025	24000603400000	Indeferido
PD26412/2025	23004102250000	Indeferido
PD26470/2025	01005705720000	Indeferido
PD26564/2025	24003801430000	Indeferido
PD27209/2025	16002403690000	Indeferido
PD27238/2025	19014900940000	Indeferido
PD27253/2025	36003103770000	Indeferido
PD27712/2025	36024901890000	Indeferido
PD27729/2025	19013100830000	Indeferido
PD27937/2025	16004600550000	Indeferido
PD27992/2025	09001702170000	Indeferido
PD28262/2025	35011502900000	Indeferido
PD29315/2025	36020402150000	Indeferido
PD31329/2025	19100001400181	Indeferido
PD32065/2025	19023902950000	Indeferido
PD32326/2025	19022800620006	Indeferido
PD32447/2025	27060001101009	Indeferido
PD32495/2025	19100001400241	Indeferido
PD32789/2025	10002603260056	Indeferido
PD32947/2025	18001302240003	Indeferido
PD32963/2025	19025003100000	Indeferido
PD33457/2025	24007904500000	Indeferido
PD33843/2025	19100001300080	Indeferido
PD33982/2025	19100001400133	Indeferido
PD34136/2025	05009207150041	Indeferido
PD34147/2025	19013600530002	Indeferido
PD34174/2025	24003802330000	Indeferido
PD34741/2025	02000502820031	Indeferido
PD35087/2025	19031300420000	Indeferido
PD35740/2025	26018201690000	Indeferido

Edital nº 115/2025 • Isenção IPTU • INDEFERIDOS Análise Definitiva

PD35801/2025	16009401890000	Indeferido
PD36099/2025	24078001100175	Indeferido
PD36177/2025	19100001300237	Indeferido
PD36761/2025	27003900930002	Indeferido
PD37236/2025	27007702910000	Indeferido
PD37632/2025	36001002960000	Indeferido
PD37671/2025	36001002900000	Indeferido
PD37687/2025	07013003020000	Indeferido
PD37922/2025	21004100760043	Indeferido
PD38218/2025	05007001850003	Indeferido
PD38527/2025	19015300860000	Indeferido
PD38620/2025	17004502960000	Indeferido
PD38932/2025	15011302990000	Indeferido
PD38975/2025	15012603280000	Indeferido
PD39113/2025	25001001280000	Indeferido
PD40635/2025	19034000310000	Indeferido
PD40705/2025	20052000300136	Indeferido
PD40763/2025	30002800600000	Indeferido
PD41242/2025	23019500130000	Indeferido
PD41580/2025	36025802460000	Indeferido
PD42030/2025	03005102170002	Indeferido
PD42265/2025	10055000210098	Indeferido
PD42743/2025	22012301400004	Indeferido
PD42940/2025	19032203570000	Indeferido
PD43256/2025	26073000300290	Indeferido
PD43340/2025	27060001100989	Indeferido
PD43442/2025	21007401010000	Indeferido
PD43576/2025	23018202100000	Indeferido
PD43680/2025	23001102650000	Indeferido
PD43931/2025	23020800380000	Indeferido
PD44097/2025	15015004090000	Indeferido
PD44109/2025	14007402750000	Indeferido
PD44183/2025	36023500550000	Indeferido
PD45087/2025	02001601550015	Indeferido
PD45817/2025	36023201160000	Indeferido
PD46063/2025	27007708720000	Indeferido
PD46147/2025	16009602880000	Indeferido
PD46264/2025	23011402650000	Indeferido
PD46270/2025	35055000820107	Indeferido
PD46291/2025	11014803290000	Indeferido
PD46319/2025	19100001300030	Indeferido
PD46324/2025	05000500650000	Indeferido
PD46326/2025	16058000510938	Indeferido
PD46635/2025	24000400330000	Indeferido
PD46860/2025	26073000280350	Indeferido
PD46983/2025	19100001400003	Indeferido
PD46992/2025	27007709910000	Indeferido
PD47008/2025	36025501550000	Indeferido
PD47254/2025	25000402920000	Indeferido
PD47449/2025	19100001400134	Indeferido
PD47719/2025	24078001100259	Indeferido
PD47776/2025	21012703740000	Indeferido

Edital nº 115/2025 • Isenção IPTU • INDEFERIDOS Análise Definitiva

PD47848/2025	19017701400000	Indeferido
PD47969/2025	26073000280356	Indeferido
PD48024/2025	04011501280009	Indeferido
PD48062/2025	36011801680000	Indeferido
PD48149/2025	11015904330000	Indeferido
PD48168/2025	27002701070000	Indeferido
PD48863/2025	22009101280000	Indeferido
PD49013/2025	16010901200000	Indeferido
PD49036/2025	27003600940000	Indeferido
PD49079/2025	19100001300221	Indeferido
PD49273/2025	26073000300258	Indeferido
PD49503/2025	11096000200872	Indeferido
PD49655/2025	35055000600182	Indeferido
PD49659/2025	17005003790000	Indeferido
PD50237/2025	15017000210000	Indeferido
PD50637/2025	19017101690000	Indeferido
PD50699/2025	16058000510716	Indeferido
PD51779/2025	36021200680000	Indeferido
PD52208/2025	20006702290003	Indeferido
PD52242/2025	36024702780000	Indeferido
PD52894/2025	15013702780000	Indeferido
PD53539/2025	11102500910194	Indeferido
PD54314/2025	21012501110000	Indeferido
PD55250/2025	08010402880000	Indeferido
PD55458/2025	19025902120000	Indeferido
PD56276/2025	27060001100938	Indeferido
PD56948/2025	19019703240000	Indeferido
PD57330/2025	09002602470000	Indeferido
PD57622/2025	06002403590000	Indeferido
PD57788/2025	26017202560001	Indeferido
PD58884/2025	19014500630000	Indeferido
PD58926/2025	15014901580000	Indeferido
PD59165/2025	13001000570000	Indeferido
PD59432/2025	18003300910000	Indeferido
PD59811/2025	25003202550000	Indeferido
PD60110/2025	11008100330000	Indeferido
PD60401/2025	16002503720001	Indeferido
PD60449/2025	19022801200000	Indeferido
PD60872/2025	36013103310000	Indeferido
PD60986/2025	20011501750006	Indeferido
PD61338/2025	19018402500000	Indeferido
PD61444/2025	24003805160000	Indeferido
PD61769/2025	19024901800000	Indeferido
PD61905/2025	01003801570018	Indeferido
PD62094/2025	19013801500000	Indeferido
PD62096/2025	19017101030000	Indeferido
PD62430/2025	24078001300009	Indeferido
PD62567/2025	19029700870000	Indeferido
PD62577/2025	26073000280184	Indeferido
PD62764/2025	13002400280000	Indeferido
PD63169/2025	26073000300092	Indeferido
PD63244/2025	19100001200003	Indeferido

Edital nº 115/2025 • Isenção IPTU • INDEFERIDOS Análise Definitiva

PD63291/2025	04004902780000	Indeferido
PD63324/2025	19019801150000	Indeferido
PD63364/2025	26073000280242	Indeferido
PD63371/2025	16058000510786	Indeferido
PD63400/2025	19026002640000	Indeferido
PD63475/2025	11005101350000	Indeferido
PD63509/2025	19002402070000	Indeferido
PD63673/2025	09003402170000	Indeferido
PD63776/2025	30003201320000	Indeferido
PD63929/2025	24005703810000	Indeferido
PD63940/2025	11011303830000	Indeferido
PD63978/2025	26073000280098	Indeferido
PD64096/2025	26073000280245	Indeferido
PD64178/2025	35003204580000	Indeferido
PD64385/2025	23003903040000	Indeferido
PD64422/2025	04006103540069	Indeferido
PD64426/2025	24078001300014	Indeferido
PD64467/2025	23007501000033	Indeferido
PD64548/2025	36002500830002	Indeferido
PD64549/2025	19002703010002	Indeferido
PD64569/2025	13006602860000	Indeferido
PD64602/2025	15014601150000	Indeferido
PD64637/2025	20007202750000	Indeferido
PD64640/2025	36009500290000	Indeferido
PD64654/2025	36002200280000	Indeferido
PD64728/2025	19100001200152	Indeferido
PD64971/2025	07005800800000	Indeferido
PD65473/2025	27001602100000	Indeferido

Prefeitura de Americana, 18 de dezembro de 2025.

ANDERSON NATEL FERREIRA
Diretor da Unidade de Julgamento de Processos Administrativos

UNIDADE DE GESTÃO FINANCEIRA

COMUNICADO N.º 71/SF/12/2025

Prezados Senhores,

Nos termos da legislação em vigor, vimos comunicar a Vossas Senhorias que houve o(s) crédito(s) a seguir discriminado(s), em benefício deste Município, oriundo(s) do governo federal.

Dia 18/12/2025 R$ 23.462,15 BANCO DO BRASIL S/A - F.N.A.S - G.B.F

Dia 18/12/2025 R$ 570.041,23 BANCO DO BRASIL S/A - SALÁRIO EDUCAÇÃO

Dia 18/12/2025 R$ 3.153,51 BANCO DO BRASIL S/A - ITA - ROYALTIES

Atenciosamente,

Americana, 19 de dezembro de 2025

KAMILE ALEXIA F. J. SOUZA
Diretora da Unidade de Tesouraria