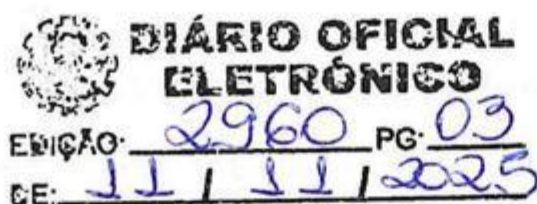




MUNICÍPIO DE ITAIPULÂNDIA

Estado do Paraná

PORTARIA Nº 844, DE 11 DE NOVEMBRO DE 2025.



Disciplina a Gestão de Identidade e Controle de Acesso e estabelece os requisitos mínimos de segurança no âmbito do ambiente tecnológico do Poder Executivo Municipal.

O PREFEITO MUNICIPAL DE ITAIPULÂNDIA, Estado do Paraná, no uso de suas atribuições legais que lhe são conferidas pela alínea "c" do Inciso II, do Art. 74, da Lei Orgânica do Município, **Resolve:**

CAPÍTULO I

DAS DISPOSIÇÕES INICIAIS

Art. 1º A Gestão de Identidade, Controle de Acesso e requisitos mínimos de segurança no âmbito do ambiente tecnológico do poder público municipal ficam disciplinados por esta Portaria.

Art. 2º A Política de Identidade e Gestão do Controle de Acesso tem como objetivo estabelecer diretrizes, competências e responsabilidades para sistematizar controles de identificação, autenticação e autorização para salvaguardar as informações do poder público municipal em meio digital, a fim de evitar a quebra de segurança da informação e quaisquer acessos não autorizados que implique em risco de destruição, alteração, perda, roubo ou divulgação indevida. Ela inclui diversos elementos, como por exemplo:

- I. identificação e autenticação de usuários;
- II. determinar quais recursos, sistemas ou informações os usuários tem permissão para acessar após a autenticação bem sucedida (definição de privilégios e níveis de acesso de acordo com as responsabilidades de cada usuário);
- III. gerenciar o acesso a sistemas, dados digitais;
- IV. estabelecer práticas para monitorar e registrar as atividades de acesso para identificar potenciais ameaças ou violações de segurança;
- V. definir diretrizes para revogar o acesso de um usuário, como por exemplo, nos casos de demissão, mudança de função ou quando o acesso se torna desnecessário para suas responsabilidades;



MUNICÍPIO DE ITAIPULÂNDIA

Estado do Paraná

- VI. envolver a conscientização de usuários sobre a importância do controle de acesso, as melhores práticas de segurança e a importância de proteger as credenciais de acesso.

§ 1º Compete ao Departamento de Tecnologia da Informação (TI) a gestão dos recursos computacionais instalados no ambiente tecnológico do órgão ou gerenciados por ele, em conformidade com os normativos vigentes e as melhores práticas de segurança da informação.

§ 2º As medidas previstas nesta instrução aplicam-se a todos os usuários do ambiente tecnológico do Poder Público Municipal, acarretando sua responsabilização em função de descumprimento, nos termos previstos em lei e demais regulamentos.

Art. 3º Para efeitos desta Portaria, considera-se:

- I. acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação do órgão ou entidade, observada eventual restrição que se aplique;
- II. ambiente tecnológico: redes, dispositivos, *softwares*, processos, informação armazenada ou em trânsito, serviços e sistemas que possam ser conectados direta ou indiretamente a redes de computadores;
- III. autenticação: processo de identificação das partes envolvidas em um processo;
- IV. autenticação multifator: autenticação realizada com a utilização de dois ou mais elementos identificadores (senha, biometria, código de acesso único, entre outros);
- V. confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;
- VI. conta de acesso: identidade digital do usuário, formalmente exercida pelo gestor técnico por meio do processo de gestão de identidade para acesso ao ambiente tecnológico (também conhecida como "usuário" ou "login");
- VII. conta de serviço: conta de acesso associada a serviço digital ou sistema, e não a usuário;
- VIII. controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos;
- IX. disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável no momento que for necessária por pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;



MUNICÍPIO DE ITAIPULÂNDIA

Estado do Paraná

- X. gestão de identidade: atividade relacionada à criação, ao bloqueio e a contas de acesso, bem como o gerenciamento e proteção das informações que identificam um usuário no ambiente tecnológico;
- XI. gestor técnico: responsável pela sustentação de determinado sistema, conjunto de sistemas ou infraestrutura de TI, bem como a implementação do perfil de acesso ao usuário;
- XII. informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- XIII. integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- XIV. perfil de acesso: coleção de atributos e permissões que um usuário ou grupo de usuários têm no ambiente tecnológico;
- XV. senha: conjunto de caracteres (letras, números e símbolos) escolhida e memorizada pelo usuário para realização do processo de autenticação;
- XVI. usuário: indivíduo que pode acessar informações, sistemas ou serviços do ambiente tecnológico;
- XVII. usuários externos: partes, sócios proprietários, visitantes e demais usuários que não estejam vinculados ao ente; e
- XVIII. usuários internos: assessores, servidores, estagiários, bem como colaboradores, prestadores de serviço, e demais usuários que estejam formalmente vinculados ao ente.

CAPÍTULO II

DA GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO

Seção I

Da Conta de Acesso

Art. 4º O acesso a recursos do ambiente tecnológico do órgão está condicionado a:

- I. identificação do usuário por meio da sua Conta de Acesso (ou Certificado Digital);
- II. autenticação do usuário por meio da senha pessoal ou outros fatores de autenticação.



MUNICÍPIO DE ITAIPULÂNDIA

Estado do Paraná

Art. 5º A criação da Conta de Acesso, condicionada à identificação formal do usuário, será realizada por meio do processo de gestão de identidade, realizada pelo gestor técnico do Departamento de TI.

Art. 6º A Conta de Acesso será atribuída a cada usuário, de forma individual e intransferível, para uso exclusivo do seu titular.

§ 1º A Conta de Acesso deve obedecer aos seguintes requisitos:

- I. possuir identificação única; e
- II. ser gerenciada por sistema de gestão de identidades destinado a esse fim.

§ 2º Os usuários são responsáveis por todos os acessos e por todas as atividades desenvolvidas por meio da sua Conta de Acesso, podendo ser responsabilizados pelos danos decorrentes de sua má utilização.

§ 3º Caso seja detectado acesso ou atividade considerada suspeita, a Conta de Acesso poderá ser bloqueada para fins de segurança e auditoria.

§ 4º Não será permitida a criação de contas de acesso genéricas não associadas a um usuário específico, exceto em casos pontuais devidamente justificados, com duração não superior a 30 (trinta) dias.

§ 5º Caso haja necessidade de criar contas de serviço, essas deverão estar vinculadas a Contas de Acesso pertencentes a usuários internos.

Art. 7º As Contas de Acesso poderão ser temporariamente bloqueadas:

- I. automaticamente após tentativas fracassadas de acesso;
- II. quando houver a suspeita de seu comprometimento;
- III. quando identificada inatividade de 30 (trinta) dias corridos ou conforme determinação do gestor técnico; e
- IV. quando a senha não for alterada no prazo determinado.

Parágrafo único. A Conta de Acesso poderá ser reativada por manifestação do usuário, mediante justificativa endereçada ao Departamento de TI ou ao gestor técnico.

Seção II

Da senha



MUNICÍPIO DE ITAIPULÂNDIA

Estado do Paraná

Art. 8º A senha associada à Conta de Acesso deve obedecer aos seguintes requisitos:

- I. tamanho mínimo de 7 (sete) caracteres quando a autenticação multifator estiver ativada;
- II. tamanho mínimo de 14 (quatorze) caracteres quando a autenticação multifator não estiver ativada;
- III. incluir, no mínimo, uma letra maiúscula, uma letra minúscula, um número e um caractere especial (por exemplo: !@#\$%&*+<->);
- IV. não estar presente em bases de dados de vazamentos conhecidos, disponíveis publicamente na internet; e
- V. quando da alteração conveniente ou programada de senha, as duas senhas anteriores não poderão ser utilizadas;
- VI. os usuários devem evitar o uso de informações pessoais óbvias, como nomes, datas de nascimento ou informações facilmente acessíveis na criação de senha;
- VII. os usuários não devem reutilizar as senhas em diferentes contas ou serviços.

Art. 9º É vedado a qualquer usuário se apropriar ou compartilhar Conta de Acesso, senha ou Certificado Digital pertencente a terceiros.

Art. 10. As senhas deverão ser mantidas em sigilo e protegidas contra leitura em texto aberto, inclusive no sistema de gestão de identidades e demais bases internas de dados, bem como ter seu tráfego protegido por meio de canal criptografado.

Parágrafo único. O Departamento de TI poderá realizar, de forma proativa, auditoria para determinar se as senhas utilizadas pelos usuários permanecem seguras e não estão presentes em bases de dados de vazamentos conhecidos na internet.

Art. 11. A alteração da senha deve ocorrer quando houver suspeita do seu comprometimento.

§ 1º Sempre que possível deve ser definida regras para expiração regulares das senhas.

§ 2º O login e senha do usuário é de uso pessoal e intransferível, portanto é proibida sua divulgação ou compartilhamento, sob pena de serem bloqueados pela área de TI quando constatada qualquer irregularidade.



MUNICÍPIO DE ITAIPULÂNDIA

Estado do Paraná

Seção III

Da Autenticação

Art. 12. O processo de autenticação ocorrerá mediante identificação da Conta de Acesso (ou Certificado Digital) e a correta verificação da senha ou de outros fatores de autenticação exigidos pelo recurso de TI ao ser acessado.

§ 1º A autenticação multifator, sempre que possível, deve ser ativada para acessar quaisquer recursos de TI do ambiente tecnológico do órgão disponibilizados na internet.

§ 2º A autenticação simples (apenas senha) pode ser utilizada quando o usuário interno se encontra conectado à rede do órgão nos seguintes cenários:

- I. usuário presente fisicamente nas dependências do órgão e utilizando recursos de microinformática disponibilizados pelo Departamento de TI;
- II. usuário em teletrabalho acessando remotamente o ambiente tecnológico do órgão por meio de canal criptografado seguro disponibilizado pelo Departamento de TI.

Art. 13. É facultado ao gestor técnico utilizar a autenticação única do Governo Federal (acesso.gov.br) desde que a autenticação multifator esteja habilitada.

Seção IV

Da concessão do perfil de acesso

Art. 14. O gestor técnico será o responsável pela criação, bloqueio temporário e na inativação de Contas de Acesso de usuários, bem como permissões e atributos referentes ao perfil de acesso dos usuários.

§ 1º Os gestores técnicos definirão os perfis de acesso para cada usuário, sendo responsáveis por operacionalizá-los.

Art. 15. Ao final de cada semestre, gestores técnicos deverão promover auditoria nos sistemas de gestão de identidades, a fim de remover contas de acesso obsoletas e adequar os perfis de acesso dos usuários ativos.

Art. 16. A autorização de usuários deve determinar quais recursos ou informações um usuário específico está autorizado a acessar e em que extensão



MUNICÍPIO DE ITAIPULÂNDIA

Estado do Paraná

para garantir que apenas indivíduos autorizados obtenham acesso a dados ou recursos específicos.

§ 1º Controles automatizados devem ser estabelecidos para a concessão e revogação de direitos de acesso.

§ 2º Rotinas devem ser definidas, documentadas e implementados para controlar a distribuição de direitos de acesso a recursos, sistemas de informação e serviços de TI.

§ 3º Os privilégios de acesso dos usuários a ativos/recursos de TI devem ser definidos pela área de TI conjuntamente com a área requisitante ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

§ 4º O nível de acesso aos ativos institucionais, recursos e serviços de TI deve ser realizado com base em perfis que definem o nível de privilégios dos usuários.

§ 5º O acesso a informações confidenciais e restritas deve ser configurado apenas quando uma necessidade de trabalho tiver sido identificada e tal acesso aprovado pelo setor responsável pela informação.

§ 6º Quando houver mudança do usuário para outro setor ou o usuário ocupar uma nova função, os direitos de acesso à rede local devem ser atualizados, conforme solicitação do responsável pelo setor.

§ 7º Compete ao gestor da secretaria solicitar a revogação de permissão de acesso do usuário aos recursos, sistemas e serviços de TI em caso de afastamentos, alterações de lotação, localização ou desligamentos.

Seção V

Do sistema de gestão de identidades

Art. 17. O Departamento de TI deverá adotar sistema de gestão de identidades centralizado por meio do qual serão geradas as contas e senhas, e criados os perfis de acesso ao ambiente tecnológico do órgão, cujos objetivos são:

- I. eliminar a necessidade de uso de Contas de Acesso genéricas, com perfil especial ou perfil de administrador;
- II. autorizar o acesso somente aos recursos necessários, observando-se a regra de privilégio mínimo; e



MUNICÍPIO DE ITAIPULÂNDIA

Estado do Paraná

- III. eliminar Contas de Acesso redundantes, eventualmente presentes nos sistemas descentralizados ou em outros recursos de TI independentes.

§ 1º O sistema de que trata o *caput* deste artigo deverá atender, ao menos, os seguintes requisitos:

- I. permitir cadastramento de informações do usuário;
- II. suportar acesso embasado em papéis ou na função "Role Based Access" (RBAC);
- III. definir diferentes níveis de privilégio de acesso para um usuário;
- IV. vincular um usuário a um ou a mais papéis;
- V. possuir interface gráfica de gerenciamento;
- VI. suportar protocolos seguros de comunicação para transporte de dados de autenticação;
- VII. gerir os acessos conforme seu ciclo de vida: ativo, inativo, revogado e cancelado.

§ 2º Mediante solicitação formal, o Departamento de TI poderá conceder, em caráter excepcional e de forma temporária, Conta de Acesso com perfil especial ou de administrador para a execução de atividade pontual tecnicamente fundamentada.

§ 3º O Departamento de TI poderá manter dois sistemas de gestão de identidades independentes, um para usuários internos e outro para usuários externos.

Seção VI

Do acesso à rede cabeada, sem fio e remota e do acesso à Internet

Art. 18. A utilização da rede cabeada e sem fio do órgão é permitida por meio de dispositivos eletrônicos providos e homologados pelo Departamento de TI, após o usuário se submeter ao procedimento de autenticação.

§ 1º O Departamento de TI poderá autorizar o ingresso na rede cabeada e sem fio de dispositivos eletrônicos particulares de usuários internos do órgão.

§ 2º O Departamento de TI poderá proceder verificação técnica de segurança nos dispositivos eletrônicos que ingressarem na rede cabeada e sem fio, podendo negar o acesso aos dispositivos que representem potencial risco ao ambiente tecnológico do órgão.



MUNICÍPIO DE ITAIPULÂNDIA

Estado do Paraná

Art. 19. Somente será permitido o acesso remoto ao ambiente tecnológico do órgão por meio de autenticação multifator, de acordo com as configurações e exigências do Departamento de TI.

§ 1º O acesso remoto ao ambiente tecnológico do órgão deve ser provido por meio de canal criptografado seguro.

Art. 20. O acesso aos serviços disponibilizados na Internet será provido pelo Departamento de TI aos usuários para o cumprimento de suas atribuições e obedecendo ao princípio de privilégio mínimo.

Art. 21. O acesso a serviços que não sejam comuns a todos os usuários, como, por exemplo, acesso a sítios, deverá ser precedido de solicitação formal, com a devida justificativa, e da respectiva autorização do gestor, diante de parecer técnico emitido pela Departamento de TI.

Art. 22. É proibido o acesso a sítios de conteúdos diversos dos compatíveis com as atribuições do usuário, incluindo aqueles que tratem de propaganda comercial ou política, sexo, pornografia, pedofilia, erotismo e assuntos correlatos, técnicas e ferramentas para invasão e evasão de sistemas, racismo, compartilhamento de arquivos, bem como de qualquer conteúdo de natureza duvidosa ou ofensiva ou que possa prejudicar o acesso legítimo a sítios utilizados para a devida prestação jurisdicional.

Art. 23. O Departamento de TI utilizará softwares específicos que efetuarão o registro de todos os acessos aos serviços providos na Internet, assim como o bloqueio aos sítios especificados no artigo anterior.

Art. 24. Em caso da necessidade de liberação de algum sítio, deverá ser enviada solicitação formal ao Departamento de Tecnologia da Informação, justificando a necessidade do desbloqueio.

Seção VII

Do monitoramento e da auditoria

Art. 25. As atividades de acesso dos usuários devem ser registradas e monitoradas para detectar atividades suspeitas ou não autorizadas e garantir a conformidade com as políticas de segurança, identificar possíveis ameaças ou atividades suspeitas, e permitir uma análise detalhada das ações realizadas.



MUNICÍPIO DE ITAIPULÂNDIA

Estado do Paraná

§ 1º Um procedimento padronizado para revisão e auditoria periódica dos logs de acesso deve ser estabelecido, documentado e mantido atualizado continuamente.

§ 2º Análise e controle de acesso aos ativos, recursos e serviços de TI devem ser realizadas em intervalos regulares para validar se todos os privilégios estão autorizados para a execução de atividades de cada função.

§ 3º Auditorias de tentativas de acesso aos ativos, recursos, sistemas e serviços de TI devem ser realizados em intervalos regulares para detectar atividades não autorizadas ou tentativas de comprometimento.

§ 4º O monitoramento e auditoria deve envolver:

- I. o registro de atividades dos usuários;
- II. a análise dos registros de atividades para identificar padrões incomuns ou atividades suspeitas;
- III. configuração de alertas para notificar imediatamente a equipe de segurança sobre atividades suspeitas ou violações de políticas de acesso;
- IV. realização de auditorias periódicas para revisar e avaliar os registros de atividades, garantindo conformidade com a política de segurança da informação e legislação pertinente;
- V. verificação regular dos privilégios de acesso dos usuários para garantir que estejam alinhados com suas funções atuais, evitando acessos desnecessários que possam representar riscos de segurança.

Seção VIII

Dos usuários

Art. 26. Compete aos usuários:

- I. atender aos princípios e diretrizes contidos nesta política, incluindo normas e procedimentos complementares destinados à segurança da informação e comunicação;
- II. guiar-se pelos princípios de confidencialidade, autenticidade, integridade, não repúdio, conformidade, controle de acesso e disponibilidade no decorrer de suas atividades;



MUNICÍPIO DE ITAIPULÂNDIA

Estado do Paraná

- III. interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo;
- IV. informar ao setor de TI qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros;
- V. zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos;
- VI. não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;
- VII. não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;
- VIII. utilizar corretamente os ativos de TI e conservá-los conforme os cuidados e medidas preventivas estabelecidas;
- IX. não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo as como pessoais e intransferíveis;
- X. solicitar uma senha, quando do esquecimento;
- XI. evitar o registro de senhas em qualquer meio;
- XII. alterar a senha sempre que existir qualquer indicação de possível comprometimento de sua confidencialidade;
- XIII. criar senhas que sejam fáceis de lembrar, mas que não sejam baseadas em elementos que outras pessoas ou possíveis invasores possam facilmente adivinhar, ou deduzir, a partir de informações pessoais;
- XIV. alterar a senha em intervalos regulares e evitar a reutilização de senhas antigas;
- XV. selecionar senhas de boa qualidade, evitando o uso de senhas muito curtas ou muito longas, que o obrigue a registrá-la em qualquer outro meio para não serem esquecidas;
- XVI. encerrar as sessões ativas ou utilizar-se do mecanismo de bloqueio de acesso (tela de proteção com senha) quando precisar se afastar dos equipamentos, mesmo que seja por um período curto.

Seção IX

Da área de Tecnologia da Informação

*Rua São Miguel do Iguaçu, 1891 – Centro – Fone: (45) 3559-8000
CEP 85.880-000 – Itaipulândia - PR - CNPJ: 95.725.057/0001-64*



MUNICÍPIO DE ITAIPULÂNDIA

Estado do Paraná

Art. 27. São obrigações da Área de Tecnologia da Informação:

- I. realizar, com a periodicidade necessária, cópias de segurança dos dados armazenados nos compartilhamentos de rede, precavendo-se quanto a catástrofes;
- II. assegurar o pleno e efetivo funcionamento dos recursos de Tecnologia da Informação e Comunicação disponibilizados;
- III. assegurar a integridade e disponibilidade dos ativos que se encontram no seu ambiente computacional;
- IV. realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação que se encontram no ambiente computacional;
- V. elaborar o Plano de Resposta a Incidentes;
- VI. manter registro das atividades de usuários (logs), de maneira a abranger o máximo de ações possíveis dentro dos sistemas e pelo maior tempo possível;
- VII. adotar como padrão de endereço de e-mail corporativo o formato @itaipulandia.pr.gov.br;
- VIII. priorizar o uso institucional do acesso à internet, podendo bloquear e/ou limitar acesso a determinados sítios de Internet e estabelecendo categorias passíveis de acesso em horários restritos;
- IX. instalar sistemas operacionais nos computadores de sua Unidade devidamente licenciados e mantê-los atualizados;
- X. instalar itens de softwares e mecanismos de proteção (minimamente, anti-vírus e firewall nas estações de trabalho) devidamente licenciados e mantê-los atualizados;
- XI. instalar e permitir a instalação apenas de software devidamente licenciado e homologado, de modo a não comprometer a segurança do ambiente;
- XII. manter atualizados e licenciados os sistemas e demais itens de software do parque computacional.

CAPÍTULO III

DO SISTEMA CONTÁBIL

Seção I

*Rua São Miguel do Iguaçu, 1891 – Centro – Fone: (45) 3559-8000
CEP 85.880-000 – Itaipulândia - PR - CNPJ: 95.725.057/0001-64*



MUNICÍPIO DE ITAIPULÂNDIA

Estado do Paraná

Requisitos de segurança do sistema

Art. 28. O sistema contábil deverá possuir mecanismos de controle de acesso de usuários baseados, no mínimo, na segregação das funções de execução orçamentária e financeira, de controle e de consulta.

§ 1º O acesso ao sistema para registro e consulta aos documentos apenas será permitido após o cadastramento e a habilitação de cada usuário, com código próprio, nos termos previstos na Seção I, II e III desta Portaria.

Art. 29. O registro das operações de inclusão, exclusão ou alteração de dados efetuadas pelos usuários será mantido no sistema e conterà, no mínimo:

- I. código do usuário;
- II. operação realizada; e
- III. data e hora da operação.

Parágrafo único. Para fins de controle, a consulta aos registros das operações a que se refere o caput estará disponível com acesso restrito a usuários autorizados.

Art. 30. Caso seja disponível a realização de operações de inclusão, exclusão ou alteração de dados no sistema via sítio na Internet, este deverá garantir sua autenticidade através de conexão segura.

Art. 31. A base de dados do sistema deverá possuir mecanismos de proteção contra acesso direto não autorizado.

§ 1º O acesso direto à base será restrito aos administradores responsáveis pela manutenção do sistema e condicionado à assinatura de termo de responsabilidade específico.

§ 2º Fica vedado aos administradores referidos no § 1º, sujeitando à responsabilização individual:

- I. divulgar informações armazenadas na base de dados do sistema; e
- II. alterar dados, salvo para sanar incorreções decorrentes de erros ou mal funcionamento do sistema, mediante expressa autorização do responsável pela execução financeira e orçamentária, observado o art. 30 desta Portaria.

Art. 32. Deverá ser realizada cópia de segurança periódica da base de dados do sistema que permita a sua recuperação em caso de incidente ou falha, sem prejuízo de outros procedimentos.



MUNICÍPIO DE ITAIPULÂNDIA

Estado do Paraná

Seção I

Requisitos contábeis do sistema

Art. 33. O sistema deverá ser desenvolvido em conformidade com as normas gerais para consolidação das contas públicas editadas pelo órgão central de contabilidade da União, relativas à contabilidade aplicada ao setor público e à elaboração dos relatórios e demonstrativos fiscais;

Art. 34. O sistema deverá permitir o registro, de forma individualizada, dos fatos contábeis que afetem ou os atos que possam afetar a gestão fiscal, orçamentária, patrimonial, econômica e financeira.

Art. 35. O sistema deverá conter rotinas para a realização de correções ou anulações por meio de novos registros, assegurando a inalterabilidade das informações originais incluídas após sua contabilização, de forma a preservar o registro histórico de todos os atos.

Art. 36. O sistema, a partir dos registros contábeis, deverá:

- I. gerar, em conformidade com o Plano de Contas Aplicado ao Setor Público aprovado pela Secretaria do Tesouro Nacional, o Diário, o Razão, e o Balancete Contábil;
- II. permitir a elaboração das demonstrações contábeis, dos relatórios e demonstrativos fiscais, do demonstrativo de estatística de finanças públicas e a consolidação das contas públicas.

Parágrafo único. Dos documentos de que trata este artigo, constarão a identificação do sistema, a unidade responsável, a data e a hora de sua emissão.

Art. 37. Para fins do cumprimento do disposto no artigo anterior e em conformidade com os prazos previstos no § 3º do art. 165 da Constituição Federal e no § 2º do art. 55 da Lei Complementar nº 101, de 4 de maio de 2000, o sistema ficará disponível:

- I. até 31 de dezembro, para registro de atos de gestão orçamentária, financeira e patrimonial relativos ao exercício financeiro;
- II. até o último dia do mês para ajustes necessários à elaboração dos balancetes do mês imediatamente anterior;
- III. até 30 de janeiro, para ajustes necessários à elaboração das demonstrações contábeis do exercício imediatamente anterior.

§ 1º Ressalvado o disposto no art. 36 desta Portaria, o sistema deverá impedir registros contábeis após o balancete encerrado.



MUNICÍPIO DE ITAIPULÂNDIA

Estado do Paraná

CAPÍTULO IV DAS PENALIDADES

Art. 38. Ações que violem esta política, norma interna complementar, procedimentos, ou que comprometem os controles de segurança da informação relacionados à controle de acesso serão passíveis de investigação, podendo implicar em penas e sanções legais impostas por meio de medidas administrativas, sem prejuízo das demais medidas cíveis e penais cabíveis.

§ 1º Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas de acesso a ativos/serviços de informação ou recursos computacionais será tratada como um incidente de segurança da informação, cabendo uma análise da infração pelo Departamento de Tecnologia da Informação e aplicação das sanções e punições previstas na legislação pertinente.

§ 2º Em situação em que haja suspeita de quebra da segurança da informação, colocando em risco os serviços ou recursos de tecnologia, a área de Tecnologia da Informação conduzirá a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

§ 3º Nos casos em que o responsável pela violação de segurança for um usuário, a área de Tecnologia da Informação comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis.

§ 4º O procedimento para a aplicação das penalidades e/ou sanções seguirá o rito específico da legislação, norma, regimento ou resolução a que corresponder o caso concreto.

CAPÍTULO IV DAS DISPOSIÇÕES FINAIS

Art. 39. O uso inapropriado dos recursos pelos usuários é passível de apuração de responsabilidade, nos termos da legislação aplicável, podendo o Departamento de TI suspender imediatamente o acesso concedido.

Parágrafo único. A suspensão será comunicada pelo setor de TI para o usuário e, quando for o caso, para o titular da unidade administrativa a qual o usuário é associado esclarecendo os detalhes da ocorrência.



MUNICÍPIO DE ITAIPULÂNDIA

Estado do Paraná

Art. 40. A inobservância dos dispositivos constantes nesta Portaria pode acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 41. As situações não previstas nesta Portaria deverão ser resolvidas pelo Departamento de Tecnologia da Informação.

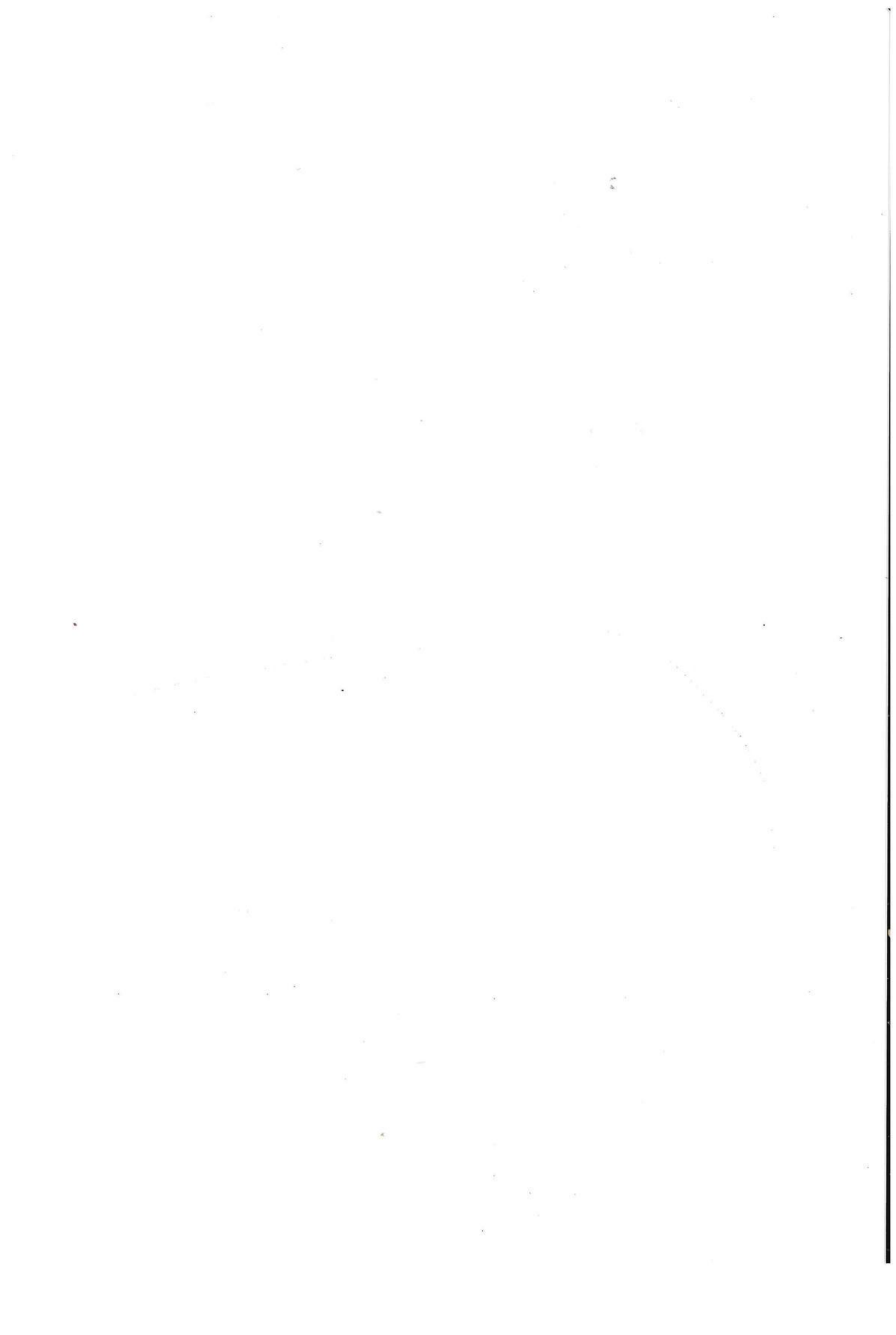
Art. 42. Esta Portaria deverá ser revisada bianualmente ou quando necessário.

Art. 43. Esta Portaria entra em vigor na data de sua publicação.

Itaipulândia, 11 de novembro de 2025.

Lindolfo Martins rui
Prefeito Municipal

Laércio Gilmei Wolmuth
Secretário de Administração





PREFEITURA MUNICIPAL DE ITAIPULÂNDIA

CÓDIGO DE AUTENTICIDADE: 8b161475-ca1f-45dc-b581-4ba9ae7ceab1



PROTOCOLO DE ASSINATURAS

O documento **PORTARIA Nº 844 - Gestão de identidade e controle de acesso.pdf** foi assinado eletronicamente através do Printer Flow. Verifique as assinaturas em

<https://itaipulandia.printercloud.com.br/signatures/eyJhbGciOiJIUzI1NiJ9.eyJ0YXNrlj0zNDUxODI9.pfiqc187FdwKx1y8vMomyMbwP1WUcOLGhBb-0akPPVg>

ou escaneie o qr code ao lado.

Lista de assinantes

Assinado por: **LAERCIO GILMEI WOLMUTH**, em 11/11/2025 às 11:29:40.

Código de verificação: 834fe066-8d27-4fa2-a354-7ae1da2b1ce1

Assinado por: **LINDOLFO MARTINS RUI**, em 11/11/2025 às 15:15:06.

Código de verificação: 29865e4b-768a-4482-b9ae-ea1311bdd294



A ASSINATURA ELETRÔNICA DESTE DOCUMENTO ESTÁ AMPARADA PELO:

DECRETO Nº: 236, DE 28 DE AGOSTO DE 2023.