**ATO NORMATIVO Nº 05/2025**

**DISPÕE SOBRE O CONTROLE DE ACESSO, A INTEGRIDADE DOS DADOS E A SEGURANÇA DO USO DO SISTEMA DE EXECUÇÃO ORÇAMENTÁRIA E FINANCEIRA MUNICIPAL.**

O PREFEITO MUNICIPAL DE IPORÃ – PR, no uso de suas atribuições legais, com fundamento nos arts. 37 e 70 da Constituição Federal, no art. 48 da Lei Complementar nº 101/2000 (Lei de Responsabilidade Fiscal), nos princípios da administração pública, e considerando:

- A necessidade de assegurar **eficiência, integridade, rastreabilidade e transparência** na gestão das finanças públicas municipais;
- As diretrizes da **Lei nº 14.129/2021**, que dispõe sobre o Governo Digital e a prestação digital de serviços públicos;
- A necessidade de conformidade com os princípios e normas de segurança da informação e governança de dados públicas;

**RESOLVE:**

## CAPÍTULO I – DAS DISPOSIÇÕES GERAIS

**Art. 1º** Este Ato Normativo estabelece diretrizes, procedimentos e padrões técnicos mínimos para assegurar a segurança, integridade, rastreabilidade e controle de acesso ao Sistema de Execução Orçamentária e Financeira Municipal, com vistas à confiabilidade dos dados públicos e à conformidade com os princípios da legalidade, publicidade, eficiência, economicidade e segurança da informação.

## CAPÍTULO II – DO CADASTRAMENTO E RESPONSABILIDADES DOS USUÁRIOS

**Art. 2º** O acesso ao sistema será concedido exclusivamente a servidores e agentes públicos previamente autorizados por ato da autoridade competente, mediante formalização de termo de responsabilidade.

**§1º** O cadastro de usuários observará os princípios da segregação de funções e do mínimo privilégio, conforme disposto no art. 8º da Instrução Normativa SEGES/ME nº 1/2019.

**§2º** O gestor do sistema deverá manter atualizado o cadastro de usuários, contendo nome, matrícula, CPF, função, lotação, e data de ativação/desativação do acesso.

**Art. 3º** Cada usuário é responsável pela veracidade das informações inseridas no sistema, respondendo administrativamente, civil e penalmente por eventuais omissões ou fraudes, nos termos da Lei nº 8.429/1992 (Lei de Improbidade Administrativa).

## CAPÍTULO III – DO CONTROLE DE ACESSO

**Art. 4º** O acesso ao sistema será individual, pessoal e intransferível, mediante credenciais protegidas por autenticação forte.

**§1º** É obrigatória a implementação de autenticação em dois fatores (2FA) para perfis administrativos e usuários com privilégios elevados.

**§2º** O compartilhamento de senha ou identidade digital caracteriza infração funcional e sujeitará o infrator às penalidades cabíveis.

**Art. 5º** Todos os acessos, ações e tentativas de acesso serão registrados em logs invioláveis, mantidos por período mínimo de 5 (cinco) anos, nos termos do art. 23 da Lei nº 12.527/2011.

## CAPÍTULO IV – DA INTEGRIDADE DOS DADOS

**Art. 6º** Os dados inseridos deverão estar devidamente fundamentados em documentos oficiais, atualizados e compatíveis com os lançamentos contábeis realizados, conforme determina a Lei nº 4.320/1964.

**Art. 7º** A constatação de qualquer erro ou inconsistência nos dados obriga o usuário responsável a comunicar imediatamente à chefia imediata e à unidade de tecnologia da informação para correção com registro formal.

## CAPÍTULO V – DA SEGURANÇA DAS INFORMAÇÕES

**Art. 8º** O sistema deverá estar estruturado com mecanismos de segurança cibernética conforme normas da ABNT NBR ISO/IEC 27001 (gestão de segurança da informação), incluindo:

I – **Controle de acesso lógico**, com autenticação e autorização por perfil funcional;
II – **Proteção contra malware** e outras ameaças;
III – **Criptografia** dos dados sensíveis em repouso e em trânsito.

**Art. 9º** A confidencialidade, integridade e disponibilidade das informações devem ser asseguradas por meio de soluções de backup, redundância e plano de contingência, conforme art. 8º da Lei nº 14.129/2021.

## CAPÍTULO VI – DO MONITORAMENTO E AUDITORIA

**Art. 10º** A Controladoria Interna, em conjunto com a área de Tecnologia da Informação, deverá realizar auditorias periódicas, no mínimo semestrais, para verificar conformidade com este Ato e com a legislação aplicável.

**Art. 11º** O sistema deve manter logs completos de atividades, acessos, modificações e exclusões de dados, com identificação do usuário, data, hora e IP de origem.

## CAPÍTULO VII – DA GESTÃO DO SISTEMA

**Art. 12º** A Administração Municipal designará por portaria os responsáveis pela gestão técnica e operacional do sistema, os quais responderão:

I – Pela manutenção da segurança do sistema;
II – Pela atualização tecnológica e dos controles de acesso;
III – Pelo atendimento de incidentes e pela implantação de correções.

**Art. 13º** Os responsáveis pela gestão do sistema deverão apresentar anualmente relatório de conformidade à Controladoria Interna e ao Chefe do Poder Executivo.

## CAPÍTULO VIII – DOS PARÂMETROS DE SEGURANÇA

**Art. 14º** O Sistema deverá atender aos seguintes requisitos técnicos mínimos:

**I – Autenticação Segura**

a) Senha forte (mínimo 8 caracteres, incluindo maiúscula, minúscula, número e caractere especial);
b) Autenticação multifator (2FA) para perfis administrativos;
c) Bloqueio automático após 5 tentativas mal sucedidas.

**II – Criptografia e Comunicação Segura**

a) Criptografia AES-256 para armazenamento;
b) b) Criptografia TLS para transmissão (HTTPS);
c) c) VPN para acessos externos.

**III – Gestão de Perfis e Permissões**

a) Perfis baseados em cargos/funções;
b) b) Auditoria de permissões a cada 90 dias;
c) c) Desativação imediata de perfis inativos ou exonerados.

**IV – Monitoramento e Logs**

a) Registro de eventos relevantes de segurança;
b) b) Alertas automáticos para acessos suspeitos;
c) c) Análise periódica de logs por equipe de TI.

**V – Plano de Recuperação de Desastres**

a) Backups diários e cópia em mídia externa ou em nuvem;
b) b) Testes semestrais de recuperação de dados;
c) c) Procedimento de resposta a incidentes cibernéticos.

**Art. 15º** Qualquer alteração nos mecanismos de segurança do sistema deverá ser precedida de parecer técnico da TI e autorizada formalmente pela autoridade competente.

## CAPÍTULO IX – DISPOSIÇÕES FINAIS

**Art. 16º** Os casos omissos serão resolvidos pela Secretaria Municipal de Administração e Tecnologia da Informação, ouvida a Controladoria Geral do Município.

**Art. 17º** Este Ato Normativo entra em vigor na data de sua publicação, revogando-se as disposições em contrário.

**Iporã – PR, 13 de Outubro de 2025.**

**ROBERTO DA SILVA**
Prefeito Municipal

# ANEXO I – TERMO DE RESPONSABILIDADE DO USUÁRIO DO SISTEMA

## TERMO DE RESPONSABILIDADE DE USO DO SISTEMA DE EXECUÇÃO ORÇAMENTÁRIA E FINANCEIRA MUNICIPAL

Eu, _____, matrícula nº _____, lotado(a) na Secretaria _____, CPF nº _____, DECLARO, para os devidos fins, que:

1. Fui devidamente autorizado(a) pela Administração Pública Municipal para acesso ao Sistema de Execução Orçamentária e Financeira Municipal;
2. Estou ciente de que o acesso ao sistema é individual, intransferível e protegido por senha de uso pessoal;
3. Comprometo-me a zelar pela confidencialidade da senha e pelo uso responsável do sistema, observando a legislação vigente, as normas internas da Prefeitura Municipal de Iporã e este Ato Normativo;
4. Reconheço que qualquer ação realizada com minhas credenciais será de minha responsabilidade, estando sujeito às sanções administrativas, cíveis e penais cabíveis no caso de descumprimento das normas;
5. Comprometo-me a comunicar imediatamente qualquer anomalia, falha ou acesso indevido detectado no sistema.

**Iporã – PR, ____ de _____ de 20____.**

Assinatura do Usuário: _____

Assinatura do Responsável pela Autorização: _____

# ANEXO II – MODELO DE RELATÓRIO DE AUDITORIA DE ACESSOS

## RELATÓRIO DE AUDITORIA DE ACESSOS AO SISTEMA DE EXECUÇÃO ORÇAMENTÁRIA E FINANCEIRA MUNICIPAL

**Período de referência:** //____ a //____
**Elaborado por:** _____
**Cargo/Função:** _____
**Órgão/Setor:** _____

| Data/Hora do Acesso | Nome do Usuário | CPF/Matrícula | IP de Origem | Ação Realizada | Resultado | Observações |
|---|---|---|---|---|---|---|
| 01/07/2025 08:10 | João da Silva | 123456 | 192.168.0.1 | Lançamento | Sucesso | — |
| 01/07/2025 09:15 | Maria Oliveira | 789123 | 192.168.0.15 | Exclusão | Falha | Acesso negado por permissão |

**Resumo de Acessos:**

- Total de acessos: _____
- Tentativas de acesso indevido: _____
- Acessos fora do horário previsto: _____
- Ações administrativas críticas: _____

**Conclusão e Recomendações:**

_____

_____

**Iporã – PR, ____ de _____ de 20____.**

Assinatura do Auditor Responsável: _____

# ANEXO III – PLANO DE CONTINUIDADE DE SERVIÇOS DIGITAIS

## PLANO MUNICIPAL DE CONTINUIDADE E RECUPERAÇÃO DE SERVIÇOS DIGITAIS ESSENCIAIS

**Objetivo:**
Garantir a continuidade operacional dos serviços relacionados ao Sistema de Execução Orçamentária e Financeira Municipal em caso de incidentes críticos, falhas técnicas, ataques cibernéticos ou desastres.

*1. Componentes do Plano:*

**I – Classificação de Serviços Essenciais:**

- Execução orçamentária
- Liquidação de despesas
- Pagamentos
- Emissão de relatórios fiscais e contábeis

**II – Procedimentos de Backup:**

- Backups diários automáticos armazenados localmente e em nuvem;
- Retenção mínima de 90 dias;
- Verificação semanal de integridade.

**III – Procedimentos de Recuperação:**

- Tempo máximo de recuperação (RTO): 6 horas;
- Perda máxima aceitável de dados (RPO): 1 dia útil;
- Equipe técnica responsável:
- _____

**IV – Testes de Contingência:**

- Realização de simulações semestrais com relatório de desempenho;
- Treinamento anual dos usuários-chave.

**V – Comunicação de Crise:**

- Acionamento imediato da TI;
- Notificação da Controladoria e Gabinete do Prefeito;
- Comunicação pública conforme gravidade.

# ANEXO IV – POLÍTICA MUNICIPAL DE SEGURANÇA DA INFORMAÇÃO (PMSI)

## 1. Finalidade

Estabelecer princípios e diretrizes para assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações processadas no âmbito do Sistema de Execução Orçamentária e Financeira Municipal.

## 2. Abrangência

Aplica-se a todos os usuários, servidores, colaboradores, contratados e gestores com acesso ao sistema.

## 3. Princípios Fundamentais:

- **Confidencialidade:** Acesso restrito às informações conforme perfil funcional;
- **Integridade:** Garantia de que os dados não serão alterados de forma indevida;
- **Disponibilidade:** Acesso garantido aos dados para os usuários autorizados sempre que necessário;
- **Rastreabilidade:** Registro completo de operações e modificações realizadas.

## 4. Diretrizes Gerais:

- Atualização periódica de credenciais de acesso;
- Proibição do uso de mídias removíveis não autorizadas;
- Monitoramento contínuo das conexões e tráfego do sistema;
- Denúncia obrigatória de incidentes de segurança;
- Treinamento obrigatório dos servidores ao ingressarem em setores com acesso ao sistema.

## 5. Sanções por Descumprimento:

Qualquer violação às diretrizes aqui estabelecidas poderá acarretar responsabilização administrativa, cível ou penal, nos termos da legislação vigente.