Diário Oficial



Prefeitura de Lindóia

Quinta-feira, 13 de novembro de 2025 Ano VI | Edição nº 1178

PREFEITURA DE LINDÓIA

Poder Executivo 3
Comunicados 3

Diário Oficial assinado digitalmente conforme MP nº 2.200-2, de 2001, garantindo autenticidade, validade jurídica e integridade.
Publicação Oficial do Município de Lindóia - Poder Executivo, conforme Lei Municipal 1.478, 22 de janeiro de 2020

PODER EXECUTIVO

Comunicados

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

As políticas, normas e procedimentos que visem garantir a segurança da informação devem ser prioridades no que diz respeito a busca e redução de riscos e falhas, danos e prejuízos que possam comprometer a imagem e os objetivos da Prefeitura Municipal da Estância Hidromineral de Lindoia-SP.

Desta forma, a Política de Segurança da Informação (PSI), define as diretrizes, os limites e o direcionamento para os controles que serão implantados na proteção de suas informações e responsabilidades legais para todos os servidores, usuários e terceiros que prestem serviços a Prefeitura Municipal da Estância Hidromineral de Lindoia-SP, devendo ser cumprida e aplicada em todas as áreas.

O Centro de Processamento de Dados (CPD) é responsável pela fiscalização na comunicação via fibra ótica, intranet, sistemas e pelo armazenamento, incluindo backups e processamento de informações, inclusive por meio de Data Centers, devendo processar e disponibilizar essas informações adequadamente e protegê-las contra ameaças e riscos.

1. OBJETIVO E ABRANGÊNCIA

1.1 Esta Política tem como objetivos:

a) Proteger as informações da Prefeitura Municipal de Lindoia contra acessos não autorizados, alterações, divulgações, destruições ou perdas acidentais;

b) Garantir a continuidade dos serviços públicos prestados à população;

c) Assegurar o cumprimento das legislações vigentes sobre proteção de dados e segurança da informação;

d) Estabelecer responsabilidades e boas práticas no tratamento de informações;

e) Promover a conscientização dos colaboradores sobre segurança da informação.

1.2 Esta Política aplica-se a todos os colaboradores da Prefeitura Municipal de Lindoia, incluindo servidores efetivos, comissionados, estagiários, terceirizados, prestadores de serviços e qualquer pessoa que tenha acesso às informações e recursos tecnológicos da instituição.

1.3 A Política abrange todas as formas de informação, sejam elas:

a) Digitais (arquivos eletrônicos, e-mails, bancos de dados, sistemas);

b) Físicas (documentos impressos, contratos, processos administrativos);

c) Verbais (conversas, reuniões, atendimentos).

2. CLASSIFICAÇÃO DA INFORMAÇÃO

2.1 As informações da Prefeitura Municipal de Lindoia serão classificadas conforme seu grau de sigilo e sensibilidade:

a) Pública: Informações que podem ser divulgadas ao público em geral sem restrições, conforme Lei de Acesso à Informação (Lei Federal nº 12.527/2011).

b) Interna: Informações de circulação restrita ao ambiente interno da Prefeitura, cujo acesso inadequado pode causar transtornos operacionais.

c) Confidencial: Informações sensíveis que, se divulgadas indevidamente, podem causar danos à administração, aos cidadãos ou comprometer a continuidade dos serviços públicos.

d) Restrita: Informações de acesso limitado a grupos específicos, protegidas por sigilo legal (fiscal, bancário, médico, processual) ou que envolvam dados pessoais sensíveis nos termos da Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018).

2.2 Todo colaborador deve identificar e tratar adequadamente as informações conforme sua classificação, respeitando os controles de acesso estabelecidos.

3. RESPONSABILIDADES

3.1 Da Diretoria de Administração:

a) Coordenar a implementação e manutenção da Política de Segurança da Informação;

b) Garantir recursos necessários para a segurança da informação;

c) Promover treinamentos e campanhas de conscientização;

d) Monitorar incidentes de segurança e coordenar respostas adequadas.

3.2 Da Área de Tecnologia da Informação:

a) Implementar controles técnicos de segurança (firewall, antivírus, backup, controle de acesso);

b) Realizar monitoramento contínuo da infraestrutura tecnológica;

c) Manter sistemas e equipamentos atualizados;

d) Gerenciar usuários, senhas e permissões de acesso;

e) Realizar cópias de segurança (backup) periódicas e testar sua restauração;

f) Investigar incidentes de segurança da informação.

3.3 Dos Gestores e Superiores Hierárquicos:

a) Assegurar que suas equipes conheçam e cumpram esta Política;

b) Autorizar acessos a sistemas e informações sob sua responsabilidade;

c) Comunicar imediatamente à Diretoria de Administração qualquer incidente de segurança;

d) Revisar periodicamente os acessos concedidos aos membros de sua equipe.

3.4 Dos Colaboradores:

a) Conhecer e cumprir integralmente esta Política;

b) Proteger informações confidenciais e restritas;

c) Utilizar recursos tecnológicos exclusivamente para fins profissionais;

d) Manter sigilo de senhas e credenciais de acesso;

e) Reportar imediatamente qualquer incidente ou suspeita de violação de segurança;

f) Participar de treinamentos sobre segurança da informação.

4. CONTROLE DE ACESSO

4.1 O acesso às informações e sistemas será concedido conforme o princípio do "menor privilégio", ou seja, cada colaborador terá acesso apenas às informações e recursos estritamente necessários ao desempenho de suas funções.

4.2 A concessão de acesso dependerá de autorização formal do superior hierárquico responsável pela área.

4.3 Todo acesso a sistemas, redes e informações será

identificado individualmente por meio de usuário e senha pessoais.

4.4 É expressamente proibido:

a) Compartilhar senhas e credenciais de acesso com terceiros;

b) Anotar senhas em locais visíveis ou de fácil acesso;

c) Utilizar credenciais de outros colaboradores;

d) Manter sessões abertas em computadores sem supervisão.

4.5 Os acessos serão revisados periodicamente e imediatamente revogados em casos de desligamento, transferência ou mudança de função do colaborador.

5. PROTEÇÃO DE DADOS PESSOAIS

5.1 A Prefeitura Municipal de Lindoia, no tratamento de dados pessoais, compromete-se a observar rigorosamente as disposições da Lei Geral de Proteção de Dados (LGPD - Lei Federal nº 13.709/2018).

5.2 Dados pessoais somente serão coletados, armazenados e processados quando houver base legal adequada e para finalidades específicas, explícitas e legítimas relacionadas às atribuições da administração pública.

5.3 Todo colaborador que tenha acesso a dados pessoais de cidadãos deve:

a) Tratá-los com confidencialidade e sigilo;

b) Utilizá-los exclusivamente para fins profissionais autorizados;

c) Não compartilhá-los de forma inadequada ou não autorizada;

d) Comunicar imediatamente qualquer incidente envolvendo dados pessoais.

5.4 É proibido:

a) Acessar dados pessoais sem autorização ou necessidade relacionada às atribuições profissionais;

b) Divulgar, copiar ou transferir dados pessoais para dispositivos ou sistemas não autorizados;

c) Utilizar dados pessoais para fins pessoais, comerciais ou não relacionados às funções públicas.

6. USO DE RECURSOS TECNOLÓGICOS

6.1 Os recursos de Tecnologia da Informação disponibilizados pela Prefeitura (computadores, notebooks, tablets, impressoras, smartphones, sistemas, e-mail corporativo, internet) são patrimônio público e devem ser utilizados exclusivamente para fins profissionais.

6.2 É permitido uso pessoal mínimo e ocasional desde que não prejudique a produtividade, não comprometa a segurança da informação e haja autorização expressa do superior hierárquico.

6.3 É expressamente proibido:

a) Acessar, armazenar ou transmitir conteúdo ilegal, ofensivo, pornográfico, discriminatório ou contrário aos bons costumes;

b) Instalar programas, jogos ou aplicativos sem autorização da área de T.I.;

c) Realizar download de arquivos suspeitos ou de fontes não confiáveis;

d) Conectar equipamentos pessoais à rede corporativa sem prévia autorização e registro;

e) Desativar ou burlar sistemas de segurança (antivírus, firewall);

6.4 A retirada de equipamentos de propriedade da Prefeitura somente será permitida mediante autorização formal do superior hierárquico, com registro de saída.

7. USO DE E-MAIL CORPORATIVO

7.1 O e-mail corporativo é ferramenta oficial de comunicação da Prefeitura e deve ser utilizado exclusivamente para assuntos profissionais.

7.2 É responsabilidade do colaborador:

a) Verificar regularmente sua caixa de e-mail corporativo;

b) Não enviar informações confidenciais ou sensíveis sem criptografia adequada;

c) Desconfiar de e-mails suspeitos, anexos inesperados e solicitações de senhas;

d) Não abrir anexos ou clicar em links de remetentes desconhecidos ou suspeitos;

e) Reportar imediatamente tentativas de phishing ou e-mails maliciosos.

7.3 É proibido:

a) Utilizar o e-mail corporativo para fins pessoais, comerciais ou políticos;

b) Enviar correntes, spam, propaganda não autorizada;

c) Criar contas de e-mail corporativo sem autorização formal;

d) Configurar redirecionamento automático de e-mails corporativos para contas pessoais sem autorização.

8. SEGURANÇA FÍSICA

8.1 O acesso às dependências onde estão localizados servidores, equipamentos de rede e informações sensíveis deve ser controlado e restrito a pessoas autorizadas.

8.2 Documentos físicos contendo informações confidenciais ou restritas devem ser:

a) Armazenados em locais seguros (armários trancados, arquivos com controle de acesso);

b) Descartados de forma segura (fragmentação, incineração) quando não mais necessários;

c) Não deixados expostos em mesas, impressoras ou áreas de circulação comum.

8.3 Monitores de computadores devem ser posicionados de forma a evitar visualização não autorizada de informações sensíveis.

8.4 Colaboradores devem bloquear suas estações de trabalho sempre que se ausentarem, mesmo que momentaneamente.

9. BACKUP E CONTINUIDADE

9.1 A área de Tecnologia da Informação realizará cópias de segurança (backup) periódicas de dados e sistemas críticos, conforme cronograma estabelecido.

9.2 Os backups serão armazenados em local seguro, preferencialmente fora das instalações principais (backup externo/nuvem), para proteção contra sinistros.

9.3 Testes de restauração de backup serão realizados periodicamente para garantir a integridade e disponibilidade das informações.

10. GESTÃO DE INCIDENTES DE SEGURANÇA

10.1 Considera-se incidente de segurança da informação qualquer evento que comprometa ou possa comprometer a confidencialidade, integridade ou disponibilidade das informações, incluindo:

a) Acesso não autorizado a sistemas ou informações;

b) Perda, furto ou roubo de equipamentos;

c) Vazamento de informações confidenciais;

d) Infecção por vírus ou malware;

e) Tentativas de invasão ou ataque cibernético;

f) Perda ou corrupção de dados;

g) Indisponibilidade de sistemas críticos.

10.2 Todo incidente de segurança deve ser imediatamente comunicado à Diretoria de Administração e à área de T.I., por meio dos seguintes canais:

Telefone: 19 3898-9928

E-mail: cpdservidor@lindoia.sp.gov.br

10.3 A área de T.I. investigará o incidente, tomará medidas para contenção e remediação, e documentará todas as ações realizadas.

10.4 Colaboradores envolvidos em incidentes devem cooperar plenamente com as investigações e não tomar ações que possam comprometer evidências.

11. MONITORAMENTO E AUDITORIA

11.1 A Diretoria de Administração, por meio da área de Tecnologia da Informação, reserva-se o direito de monitorar e auditar, sem necessidade de aviso prévio:

a) Uso de sistemas, aplicações e recursos de T.I.;

b) Tráfego de rede e acessos à internet;

c) E-mails corporativos enviados e recebidos;

d) Arquivos armazenados em servidores, estações de trabalho e dispositivos corporativos;

e) Registros de acesso (logs) a sistemas e informações.

11.2 O monitoramento visa assegurar a conformidade com esta Política, identificar vulnerabilidades e detectar atividades suspeitas.

11.3 Os colaboradores, ao utilizarem recursos da Prefeitura, consentem expressamente com o monitoramento descrito neste artigo.

11.4 Informações obtidas por meio de monitoramento serão tratadas com confidencialidade e utilizadas exclusivamente para fins de segurança, conformidade e investigação de incidentes.

12. TRABALHO REMOTO E DISPOSITIVOS MÓVEIS

12.1 Colaboradores autorizados a trabalhar remotamente ou utilizar dispositivos móveis corporativos devem:

a) Conectar-se à rede da Prefeitura apenas por meio de canais seguros (VPN, quando disponível);

b) Manter os dispositivos protegidos por senha ou biometria;

c) Não permitir que terceiros utilizem equipamentos corporativos;

d) Reportar imediatamente perda ou roubo de dispositivos;

e) Não armazenar informações sensíveis em dispositivos pessoais.

13. FORNECEDORES E TERCEIROS

13.1 Fornecedores, prestadores de serviços e terceiros que tenham acesso a informações ou sistemas da Prefeitura devem:

a) Cumprir todas as disposições desta Política;

b) Utilizar as informações exclusivamente para os fins contratados;

c) Devolver ou destruir informações ao término do contrato.

13.2 Contratos com terceiros devem incluir cláusulas específicas sobre segurança da informação e proteção de dados pessoais.

14. DESCARTE SEGURO DE INFORMAÇÕES

14.1 Informações em meio físico classificadas como confidenciais ou restritas devem ser descartadas quando autorizado pelo seu superior hierárquico por meio de:

a) Fragmentação (uso de fragmentadora cross-cut);

b) Incineração, quando apropriado;

c) Destinação a empresa especializada em descarte seguro.

14.2 Equipamentos de T.I. (computadores, HDs, pen drives) devem ter seus dados completamente apagados (sanitização) antes do descarte, doação ou reutilização.

14.3 A área de T.I. é responsável pela sanitização de mídias digitais, utilizando ferramentas apropriadas que garantam a irrecuperabilidade dos dados.

15. SANÇÕES E PENALIDADES

15.1 O descumprimento desta Política sujeitará o colaborador a um processo administrativo disciplinar que poderá resultar em:

a) Advertência por escrito;

b) Suspensão de acesso a sistemas e recursos de T.I.;

c) Aplicação de penalidades previstas no Estatuto dos Servidores Públicos Municipais;

d) Responsabilização civil e criminal, quando cabível.

15.2 Infrações cometidas por terceiros, prestadores de serviço ou fornecedores poderão acarretar:

a) Rescisão contratual;

b) Aplicação de multas contratuais;

c) Responsabilização civil e criminal.

15.3 A gravidade da infração será avaliada considerando:

a) Grau de comprometimento da confidencialidade, integridade ou disponibilidade das informações;

b) Impacto aos serviços públicos e aos cidadãos;

c) Intencionalidade ou negligência do infrator;

d) Reincidência.

16. DISPOSIÇÕES GERAIS

16.1 Esta Política estará permanentemente disponível para consulta:

a) No site oficial da Prefeitura Municipal de Lindoia;

c) Em cópia física no Departamento de Recursos Humanos.

16.2 O desconhecimento das disposições desta Política não eximirá o colaborador de suas responsabilidades.

16.3 Esta Política complementa e não substitui outras normas internas, legislações específicas e políticas setoriais da Prefeitura Municipal de Lindoia.

Lindoia, 13 de novembro de 2025.

JESSICA DAIANE FORMAGIO

DIRETORA DA ADMINISTRAÇÃO

.....