DECRETO Nº 23058/2026

Institui a Política de Segurança da Informação (PSI) e o Uso de Ativos de Tecnologia no âmbito do Poder Executivo Municipal de Dois Vizinhos, estabelecendo princípios, diretrizes e responsabilidades para o uso seguro e ético dos recursos tecnológicos

Luis Carlos Turatto, Prefeito de Dois Vizinhos, Estado do Paraná, no uso de suas atribuições legais,

D E C R E T A:

DISPOSIÇÕES GERAIS

Art. 1º Fica instituída, no âmbito do Poder Executivo Municipal, a Política de Segurança da Informação – PSI, observadas as diretrizes estabelecidas neste Decreto e em seus anexos.

Art. 2º A Política de Segurança da Informação aplica-se a todos os agentes que, de qualquer forma, utilizem ou tenham acesso aos ativos de tecnologia e informação da Prefeitura Municipal de Dois Vizinhos, incluindo servidores efetivos, comissionados, temporários, estagiários, menores aprendizes, prestadores de serviço e demais colaboradores.

Art. 3º Para fins deste Decreto, consideram-se Ativos de Tecnologia e Informaçãotodos os dados, informações e recursos, físicos ou digitais, utilizados para acessá-los, processá-los, armazená-los ou transmiti-los, compreendendo:

I – equipamentos, tais como computadores, notebooks, servidores, tablets, smartphones, impressoras e dispositivos de rede;

II – softwares e sistemas, incluindo sistemas de gestão (ERP), sistemas operacionais, aplicativos, bases de dados e serviços de produtividade;

III – infraestrutura, abrangendo redes cabeadas ou sem fio, links de internet, e-mail institucional e serviços em nuvem autorizados;

IV – informações, referentes a todos os dados gerados, recebidos ou armazenados pela Prefeitura, em qualquer tipo de mídia.

Art. 4º A gestão da Segurança da Informação caberá à Secretaria de Desenvolvimento Econômico, Científico e Tecnológico.

CAPÍTULO II

DA INFRAESTRUTURA FÍSICA

Art. 5º A instalação de infraestrutura de rede lógica no âmbito da Prefeitura Municipal de Dois Vizinhos, seja em edificações novas ou existentes, em layouts inéditos ou adaptados, deverá observar rigorosamente as especificações técnicas definidas pela Secretaria de Desenvolvimento Econômico, Científico e Tecnológico e dependerá de aprovação prévia do Departamento de Tecnologia da Informação.

Parágrafo único. Os projetos técnicos elaborados por qualquer órgão da Prefeitura que envolvam implantação ou adequação de redes e estruturas lógicas de tecnologia da informação deverão ser encaminhados à Secretaria de Desenvolvimento Econômico, Científico e Tecnológico para análise e aprovação do Departamento de Tecnologia da Informação.

CAPÍTULO III

PRINCÍPIOS E RESPONSABILIDADES

Art. 6º A Política de Segurança da Informação rege-se pelos seguintes princípios fundamentais:

I – confidencialidade: garantia de acesso às informações apenas por pessoas autorizadas;

II – integridade: preservação da exatidão, consistência e completude das informações e dos métodos de seu processamento;

III – disponibilidade: asseguramento de acesso às informações e aos ativos tecnológicos pelos usuários autorizados sempre que necessário;

IV – autenticidade: verificação da identidade de quem envia ou recebe a informação;

V – legalidade: observância das normas legais e regulamentares aplicáveis, especialmente da Lei Geral de Proteção de Dados – LGPD.

Art. 7º Constituem responsabilidades dos usuários dos ativos de tecnologia e informação do Poder Executivo Municipal:

I – utilizar os recursos tecnológicos de forma ética, profissional e exclusivamente para o desempenho das atribuições funcionais;

II – manter sob guarda e sigilo suas credenciais de acesso, as quais são pessoais e intransferíveis;

III – comunicar imediatamente à Secretaria de Desenvolvimento Econômico, Científico e Tecnológico qualquer incidente de segurança, incluindo perda de dispositivo, suspeita de malware ou recebimento de comunicação eletrônica maliciosa;

IV – observar integralmente as normas e diretrizes previstas nesta Política e em seus anexos;

V – assinar a Declaração de Ciência e Responsabilidade constante do Anexo I.

Art. 8º Compete aos gestores das Secretarias Municipais:

I – definir os níveis de acesso de suas equipes aos sistemas corporativos, em conformidade com o princípio da necessidade de acesso;

II – assegurar que suas equipes tenham conhecimento e cumpram as diretrizes estabelecidas nesta Política;

III – comunicar à Secretaria de Desenvolvimento Econômico, Científico e Tecnológico e ao Departamento de Recursos Humanos, imediatamente após o desligamento de colaboradores, para a pronta revogação dos respectivos acessos.

CAPÍTULO IV

DIRETRIZES DE SEGURANÇA

Art. 9º A governança e a classificação das informações no âmbito da Prefeitura Municipal observarão as seguintes diretrizes:

I – toda informação produzida, recebida ou custodiada pela Prefeitura será classificada quanto ao seu nível de sensibilidade, nas seguintes categorias:

a) Pública– informação destinada à divulgação ampla, sem restrições de acesso;

b) Interna– informação cujo acesso é restrito aos agentes públicos que dela necessitem para o desempenho de suas atribuições;

c) Confidencial–informação cujo acesso é limitado e depende de autorização específica, em razão de seu potencial impacto institucional, estratégico, operacional, financeiro ou legal;

II – norma específica, a ser editada pela Secretaria de Desenvolvimento Econômico, Científico e Tecnológico, detalhará os critérios e procedimentos para a correta classificação, rotulação, armazenamento e tratamento das informações previstas no inciso I;

III – o tratamento de dados pessoais observará integralmente a Lei Geral de Proteção de Dados – LGPD, garantindo a segurança, os direitos dos titulares e a limitação do acesso às finalidades estritamente necessárias;

IV – a cópia, o compartilhamento ou a exportação de bases de dados somente poderão ocorrer mediante autorização formal da Secretaria de Desenvolvimento Econômico, Científico e Tecnológico e para finalidades legítimas, conforme a natureza e a classificação da informação.

Art. 10. O controle de acesso aos sistemas e às redes municipais observará as seguintes regras:

I – o acesso será concedido mediante credencial única e intransferível;

II – é obrigatório o uso de senhas fortes, com requisitos de complexidade e periodicidade de troca, conforme o Anexo II - Manual de Senhas;

III – a Secretaria de Desenvolvimento Econômico, Científico e Tecnológico implementará, sempre que aplicável, autenticação multifator para acesso a sistemas críticos e serviços em nuvem;

IV – o usuário deverá bloquear a estação de trabalho sempre que se ausentar do posto.

Art. 11. O acesso às rotinas e módulos de execução orçamentária e financeira, no âmbito da Secretaria Municipal de Fazenda, e às rotinas de gestão de pessoas, no âmbito da Secretaria Municipal de Administração, dependerá de autorização prévia e formal dos respectivos Secretários Municipais ou de Diretores por eles delegados.

Art. 12. O uso do e-mail institucional, das ferramentas de comunicação e da internet observará as seguintes disposições:

I – o e-mail institucional destina-se exclusivamente às comunicações profissionais;

II – é proibida a abertura de mensagens ou links suspeitos, devendo o usuário reportar imediatamente tentativas de phishing à Secretaria de Desenvolvimento Econômico, Científico e Tecnológico;

III – é vedado o envio de mensagens com conteúdo ilegal, ofensivo, discriminatório ou contrário à legislação vigente;

IV – o acesso à internet será monitorado pela Secretaria de Desenvolvimento Econômico, Científico e Tecnológico para fins de segurança e otimização de recursos, podendo ser bloqueados sites que representem risco ou contenham material inapropriado.

Art. 13. O uso de softwares e serviços em nuvem no ambiente municipal obedecerá às seguintes regras:

I – é proibida a instalação de software não homologado pela Secretaria de Desenvolvimento Econômico, Científico e Tecnológico;

II – é vedada a utilização de serviços de armazenamento em nuvem não autorizados, devendo-se utilizar as plataformas oficiais disponibilizadas pelo Município;

III – o download de arquivos deverá restringir-se a necessidades profissionais e a fontes confiáveis.

Art. 14. O uso de dispositivos móveis e o acesso remoto observarão as seguintes diretrizes:

I – a utilização de dispositivos pessoais para acesso aos sistemas municipais poderá ser autorizada pela Secretaria de Desenvolvimento Econômico, Científico e Tecnológico, mediante instalação de solução de gerenciamento que assegure ambiente de trabalho segregado e seguro;

II – o acesso remoto à rede da Prefeitura deverá ocorrer exclusivamente por meio da VPN institucional;

III – os dispositivos portáteis fornecidos pela Prefeitura são de responsabilidade do usuário, que deverá adotar medidas de segurança física e lógica, comunicando imediatamente perda ou roubo.

Art. 15. A resposta a incidentes de segurança obedecerá às seguintes regras:

I – qualquer evento que comprometa ou possa comprometer a segurança da informação deverá ser comunicado imediatamente à Secretaria de Desenvolvimento Econômico, Científico e Tecnológico pelos canais oficiais;

II – a omissão ou tentativa de ocultar incidentes será considerada falta grave, sujeitando o infrator às penalidades cabíveis.

CAPÍTULO V

DAS VEDAÇÕES E SANÇÕES

Art. 16. É expressamente vedado aos usuários, além das demais proibições previstas nesta Política:

I – utilizar os recursos de tecnologia da informação para fins particulares, ilícitos ou alheios ao interesse público;

II – efetuar vendas ou compras online no horário de expediente, ou fora dele, utilizando-se de recursos da Administração Pública para fins alheios ao interesse público, de acordo com as compêtencias que lhe foram delegadas por autoridade superior;

III - compartilhar informações classificadas como internas ou confidenciais com pessoas não autorizadas, sejam elas integrantes ou não da Administração Municipal;

IV – realizar download ou upload de arquivos, aplicativos, softwares ou quaisquer mídias que não guardem relação direta e necessária com suas atividades profissionais;

a) incluem-se nessa vedação, entre outros, jogos, filmes, séries, músicas, aplicativos de uso pessoal e conteúdos destinados ao entretenimento;

b) excetuam-se os arquivos e aplicativos indispensáveis ao desempenho das funções do usuário, desde que o download ou upload seja expressamente autorizado pela chefia imediata ou pela Secretaria de Desenvolvimento Econômico, Científico e Tecnológico;

c) em qualquer hipótese, é proibido baixar, enviar ou compartilhar conteúdo que viole direitos autorais ou de propriedade intelectual, bem como material ilegal, malicioso, pornográfico, discriminatório ou ofensivo;

V – tentar burlar, desativar ou comprometer os sistemas de segurança, tais como firewalls, antivírus ou filtros de conteúdo;

VI – conectar dispositivos de armazenamento pessoais (pen drives, HDs externos, entre outros) sem prévia verificação de segurança e autorização da Secretaria de Desenvolvimento Econômico, Científico e Tecnológico;

VII – realizar manutenção, alteração física ou modificação de configuração dos equipamentos de TI sem autorização expressa da Secretaria de Desenvolvimento Econômico, Científico e Tecnológico;

VIII – interferir, danificar ou comprometer, de qualquer modo, o funcionamento do sistema de monitoramento por câmeras (CFTV), incluindo, mas não se limitando a:

a) danificar, destruir, remover ou desconectar câmeras, cabos, fontes de energia ou equipamentos de gravação;

b) obstruir, cobrir, sujar ou direcionar objetos que impeçam a captação das imagens;

c) alterar a posição ou o ângulo das câmeras sem autorização prévia da Segurança Patrimonial;

d) tentar praticar ou auxiliar terceiros na prática de quaisquer dessas condutas;

IX – deixar de comunicar imediatamente ao gestor imediato ou à Segurança Patrimonial qualquer dano, obstrução, mau funcionamento ou irregularidade identificada no sistema de vigilância eletrônica.

Art. 17. O descumprimento das normas desta Política de Segurança da Informação sujeitará o infrator às sanções disciplinares previstas no Estatuto dos Servidores Municipais de Dois Vizinhos, mediante processo administrativo, sem prejuízo das responsabilidades civis e criminais cabíveis.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 18. A Secretaria de Desenvolvimento Econômico, Científico e Tecnológico poderá promover, treinamentos e campanhas de conscientização destinados a todos os usuários, com o objetivo de reforçar boas práticas de segurança da informação e incentivar a cultura institucional de proteção de dados.

Art. 19. A Secretaria de Desenvolvimento Econômico, Científico e Tecnológico poderá monitorar o tráfego de rede, acessar registros de sistemas e realizar auditorias em equipamentos corporativos, a qualquer tempo e sem aviso prévio, exclusivamente para garantir a observância desta Política e a segurança do ambiente tecnológico da Administração. Tais ações deverão observar integralmente a legislação aplicável, especialmente as normas de proteção de dados pessoais.

Art. 20. Esta Política será revisada sempre que circunstâncias extraordinárias justificarem atualização, assegurando sua compatibilidade com novas tecnologias, ameaças emergentes e alterações normativas.

Art. 21. Os casos omissos serão analisados e decididos pela Secretaria de Desenvolvimento Econômico, Científico e Tecnológico, que poderá expedir orientações complementares quando necessário.

Art. 22. Revoga-se o Decreto n° 20271/2024.

Art. 23. Este Decreto entra em vigor em 29 de janeiro de 2026, revogando-se as disposições em contrário.

Gabinete do Executivo Municipal de Dois Vizinhos, Estado do Paraná, aos vinte e nove dias do mês de janeiro do ano de dois mil e vinte e seis, 65º ano de emancipação.

Luis Carlos Turatto
Prefeito

Registre-se
Publique-se
Cumpra-se

Dione Luiz da Silva
Secretário de Administração e Finanças

ANEXO I

DECLARAÇÃO DE CIÊNCIA E RESPONSABILIDADE

Eu,_____, matrícula nº _____, CPF nº _____, declaro ter recebido, lido e compreendido integralmente os termos da Política de Segurança da Informação (PSI) instituída pelo Decreto Municipal nº 23058/2026.

Estou ciente de minhas responsabilidades quanto ao uso ético e seguro dos ativos de tecnologia e informação da Prefeitura Municipal de Dois Vizinhos, incluindo a proteção de minhas credenciais de acesso e a obrigação de reportar quaisquer incidentes de segurança.

Concordo em cumprir todas as diretrizes estabelecidas e reconheço que o não cumprimento implicará na aplicação das sanções disciplinares cabíveis, conforme a legislação vigente.

Autorizo, por meio deste, o monitoramento do uso dos recursos tecnológicos que me forem disponibilizados, para os fins de segurança previstos na PSI.

Dois Vizinhos/PR, ___ de _____ de 20___.

_____

Assinatura do Servidor

ANEXO II

POLÍTICA DE USO E PROTEÇÃO DE SENHAS

1. Objetivo

O objetivo desta política é estabelecer um padrão para o uso seguro e a proteção de todas as senhas relacionadas ao trabalho.

2. Aplicação e Responsabilidade

Esta política é aplicável a todos os funcionários, prestadores de serviços, consultores, trabalhadores temporários e outros, incluindo todo o pessoal afiliado a terceiros. Esta diretriz se aplica a todas as senhas, incluindo, entre outras, contas de nível de usuário, contas de nível de sistema, contas da Web, contas de e-mail, proteção de proteção de tela, correio de voz e logins de roteador local.

3. Definições

Credencial: qualquer forma de prova ou evidência que serve para autenticar a identidade de um indivíduo ou a autoridade de um sistema, permitindo o acesso a recursos ou informações restritas.

Criptografia: é um mecanismo de segurança e privacidade que torna determinada comunicação (textos, imagens, vídeos e etc) ininteligível para quem não tem acesso aos códigos de "tradução" da mensagem.
MFA: A autenticação multifator (MFA) é um processo de login de conta com várias etapas que obriga o usuário a inserir informações que vão além de uma simples senha. Por exemplo, juntamente com a senha, os usuários podem ser solicitados a inserir um código que foi enviado para o e-mail deles, responder a uma pergunta secreta ou verificar uma impressão digital. Em caso de comprometimento de uma senha do sistema, uma segunda forma de autenticação pode ajudar a impedir o acesso não autorizado à conta.

4. Procedimento

4.1. Requisitos Senhas fortes: São longas; quanto mais caracteres uma senha tiver, mais forte ela será.

Recomendação: Mínimo de 8 caracteres em todas as senhas relacionadas ao trabalho.

Incentiva-se: O uso de frases-senha, senhas compostas de várias palavras. Justifica-se esse procedimento pois, as frases-senha são fáceis de lembrar e digitar, mas atendem aos requisitos de força.

Senhas para usuário e para o sistema: Todas devem estar em conformidade com as Diretrizes de Senhas moderadas, compostas por 8 caracteres, incluindo números, letras maiúsculas e minúsculas, e símbolos especiais.

Restrições do Sistema: Nos casos em que o sistema não obrigue o uso de senhas com no mínimo 8 caracteres, cabe ao colaborador assegurar que essa prática seja adotada.

Gerenciadores de Senhas: Os usuários estão autorizados a utilizar gerenciadores de senhas como (KeePass, Dashlane), que armazenam e gerenciam de forma segura todas as suas senhas relacionadas ao trabalho.

Senha Errada: Após cinco tentativas fracassadas de login, a conta será bloqueada por pelo menos 15 minutos.

4.2. Troca das Senhas

Troca obrigatória: As senhas devem ser alteradas sempre que houver indícios de comprometimento ou caso não estejam em conformidade com os requisitos de criação de senha.

Expiração das senhas: As senhas de credenciais usadas para acessar a rede ou as aplicações serão reiniciados automaticamente a cada 180 dias.

Senhas novas: Os sistemas de informação registrarão um histórico das últimas quatro senhas utilizadas por cada usuário, proibindo a reutilização dessas senhas para garantir uma maior segurança.

4.3. Proteção de Senhas

Pessoalidade: Cada conta de acesso é pessoal e intransferível, destinada exclusivamente ao usuário designado.

Responsabilidade: O usuário é totalmente responsável por todas as atividades realizadas através de sua conta, incluindo quaisquer violações ou atos ilícitos, mesmo que executados por terceiros que tenham acesso à mesma.

Não se recomenda: Evite usar nomes, sobrenomes, nomes de familiares ou colegas de trabalho, bem como qualquer informação pessoal facilmente acessível, como placas de carro, datas de aniversário ou endereços, nas suas senhas.

Senhas não autorizadas: Não é possível usar repetições ou sequências de caracteres, números ou letras.

Não gerar senha: Não inclua qualquer parte ou variação dos nomes das Secretarias Municipais e/ou Prefeitura nas suas senhas.

Senhas proibidas: É proibido utilizar senhas associadas ao trabalho em contas pessoais.

Informe imediatamente: A equipe de segurança deverá ser comunicada imediatamente, caso se detecte qualquer falha ou vulnerabilidade que possa permitir o uso não autorizado de ativos de informação, sistemas ou recursos computacionais das Secretarias Municipais e/ou Prefeitura.

Guarda das Senhas: As senhas não devem ser inseridas em mensagens de e-mail ou outras formas de comunicação eletrônica, nem reveladas por telefone a ninguém.

Recursos que não devem ser utilizados: Não use o recurso "Lembrar senha" nos aplicativos (por exemplo, navegadores da Web).

Autenticação multifatorial (MFA): é altamente recomendada e deve ser usada sempre que possível, não apenas para contas relacionadas ao trabalho, mas também para contas pessoais.

4.4. Os desenvolvedores de aplicativos devem garantir que seus programas contenham as seguintes precauções de segurança: Os aplicativos devem oferecer suporte à autenticação de usuários individuais, não de grupos.
Os aplicativos não devem armazenar senhas em texto claro ou em qualquer forma facilmente reversível.
Os aplicativos não devem transmitir senhas em texto claro pela rede.
Os aplicativos devem fornecer algum tipo de gerenciamento de funções, de modo que um usuário possa assumir as funções de outro sem precisar saber a senha do outro.

4.5. Senhas de Uso Privilegiado
Todas as contas privilegiadas (ex: administrator, root, etc.) devem ter as senhas trocadas, renomeadas e desabilitadas.
Os acessos privilegiados, por questões de segurança, devem ser realizados por uma quantidade mínima de usuários, que terão perfis de administradores e autorização de acesso para essas funcionalidades.
Caso as contas privilegiadas não possam ter as senhas trocadas ou renomeadas, serão desabilitadas e consideradas "contas de serviço" não sendo utilizadas para qualquer tipo de acesso.
As senhas não devem ser introduzidas em linhas de comando (códigos fontes) e ou em scripts abertas, mas, caso seja necessário, devem ser criptografadas se consideradas "contas de serviço".
Todas senhas em trânsito, ou seja, que sejam trafegadas pela rede obrigatoriamente deverão estar encriptadas.

5. Política de Conformidade

5.1. Medição de Conformidade: A equipe de Segurança da Informação verificará a conformidade com essa política por meio de vários métodos, incluindo, entre outros, relatórios de ferramentas de negócios, auditorias internas e externas e feedback para o proprietário da política.

5.2. Exceções: Qualquer exceção à política deve ser aprovada com antecedência pela equipe de Segurança da Informação.

5.3. Não Conformidade: Um funcionário que tenha violado esta política pode estar sujeito a medidas disciplinares, incluindo a rescisão do contrato de trabalho.