PUBLICADO EM BOLETIM OFICIAL
Nº 7531 DE 20/12/2024

DECRETO Nº 8.835, DE 18 DE DEZEMBRO DE 2024.

Dispõe sobre a Política da Segurança da Informação que trata das diretrizes e regras gerais de recursos tecnológicos no âmbito da Prefeitura Municipal de Duque de Caxias.

O PREFEITO DO MUNICÍPIO DE DUQUE DE CAXIAS, no uso da atribuição que lhe confere a Lei Orgânica Municipal;

Considerando o Processo Administrativo nº 003/003355/2024;

Considerando que a Prefeitura Municipal de Duque de Caxias utiliza-se de recursos de tecnologia da informação para seu funcionamento, onde dados relevantes e pessoais são tratados, devendo tais recursos serem utilizados com a devida segurança e integridade;

Considerando o disposto no capítulo VII da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados);

Considerando o disposto na Lei Municipal nº 3.385, de 13 de março de 2024, que estabelece medidas para o processo de adequação à Lei Nacional de Proteção de Dados no âmbito do Poder Executivo Municipal de Duque de Caxias.

DECRETA:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Ficam definidas nesta Política, as diretrizes e regras gerais para garantia de segurança da informação na Prefeitura de Duque de Caxias.

Art. 2º São objetivos da Política de Segurança da Informação:

I - estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;

II - estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos inerentes à estrutura de tecnologia da informação, limitando-os a níveis

aceitáveis, bem como auxiliar na preservação dos princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações;

III - estabelecer competências e responsabilidades quanto à segurança da informação;

IV - nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação;

V - promover o alinhamento das ações de segurança da informação com as estratégias de planejamento organizacional do Poder Executivo Municipal.

Art. 3º As ações de segurança da informação da PMDC são norteadas pelos princípios constitucionais e administrativos que norteiam a Administração Pública, bem como pelos seguintes:

I – disponibilidade, integridade, confidencialidade e autenticidade das informações;

II – continuidade dos processos e serviços essenciais para o funcionamento da PMDC;

III – economicidade da proteção dos ativos de informação;

IV - respeito ao acesso à informação, à proteção de dados pessoais e à privacidade;

V – observância da publicidade como preceito geral e do sigilo como exceção;

VI – responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação;

VII – alinhamento estratégico da Política de Segurança da Informação com o planejamento estratégico da PMDC, assim como demais normas específicas de segurança da informação da Administração Pública Municipal;

VIII – conformidade das normas e das ações de segurança da informação com a legislação regulamentos aplicáveis;

IX – educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.

Art. 4º A Subsecretaria de Tecnologia da Informação e Modernização Administrativa (SUBTIMA) da Secretaria Municipal de Governo é o setor responsável pela administração dos recursos tecnológicos do executivo municipal, sendo esse também incumbido de definir, garantir a execução e monitorar, os procedimentos de segurança da informação em âmbito municipal, além das seguintes atribuições:

I - facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos na PMDC, em conjunto com o Gestor do órgão em que for originado o incidente, e a Comissão Permanente de Proteção de Dados;

II - monitorar as redes computacionais;

III - detectar e analisar ataques e intrusões;

IV - tratar incidentes de segurança da informação;

V - identificar vulnerabilidades e artefatos maliciosos;

VI - recuperar sistemas de informação;

VII - promover a cooperação com outras equipes, participar de fóruns e redes relativas à segurança da informação, promover treinamentos e capacitações para utilização de tecnologias, bem como a orientação quanto às medidas de segurança cibernética na PMDC.

Parágrafo único. Cada Secretaria Municipal e Procuradoria-Geral, que possuir equipe técnica de T.I., deverá atribuir a esses as responsabilidades inerentes à segurança da informação, elencadas nos incisos anteriores, podendo a SUBTIMA orientar, caso seja solicitado, sobre as melhores práticas no segmento.

CAPÍTULO II

IDENTIFICAÇÃO DE USUÁRIO E SENHA DE ACESSO

Art. 5º O login de rede e a senha associada serão atribuídos a um setor específico e devem ser de uso exclusivo, não podendo ser compartilhados entre setores.

§ 1º O login e senha compõem a identidade do setor na rede corporativa, sendo vedada a sua divulgação a terceiros.

§ 2º As credenciais de acesso são geradas de acordo com um padrão estabelecido, e sua escolha não é permitida.

§ 3º Cada usuário é responsável pelas suas próprias ações, incluindo qualquer dano e violações causadas por seu uso inadequado.

§ 4º Apenas os que forem definidos como administradores dos recursos tecnológicos serão responsáveis por conceder permissões de acesso.

Art. 6º As estratégias de segurança por restrição e controle de acesso devem ser permitidas pela SUBTIMA, sendo gerenciadas apenas por pessoas devidamente autorizadas.

CAPÍTULO III

USO DAS ESTAÇÕES DE TRABALHO

Art. 7º As estações de trabalho, compostas geralmente por computadores completos, sendo desktop ou notebook, devem ser utilizadas com responsabilidade e para fins profissionais.

§ 1º É proibido acessar e manter conteúdos inapropriados como pornografia, discriminação, jogos e afins, nos servidores e estações de trabalho.

§ 2º Todos os recursos tecnológicos disponibilizados devem ser zelados pelo usuário, garantindo sua integridade e segurança.

§ 3º Quaisquer intervenções técnicas nas estações de trabalho, deverão ser realizadas pela SUBTIMA na presença dos usuários, salvo em casos que houver necessidade de realizar manutenção em laboratório técnico contendo prazo para devolução ao usuário.

§ 4º A SUBTIMA pode realizar diagnósticos e verificar arquivos de computadores e servidores, com o consentimento do usuário, especialmente em caso de suspeita de violação de regras.

§ 5º A estação de trabalho deve ser bloqueada pelo usuário sempre que este se ausentar para proteger informações.

§ 6º Os backups de dados diretamente nas estações de trabalho são responsabilidade do usuário, ficando a cargo da SUBTIMA os backups de armazenamento nos servidores computacionais gerais.

§ 7º Qualquer suporte remoto na estação de trabalho só pode ser realizado por técnicos autorizados da SUBTIMA.

§ 8º Em caso de transferência, licença, aposentadoria ou exoneração, o usuário deve devolver qualquer equipamento da PMDC sob sua responsabilidade.

Art. 8º O compartilhamento de diretórios, arquivos e outros recursos utilizados internamente para fins profissionais, só pode ocorrer com a autorização prévia da SUBTIMA, devido aos riscos de contaminação com softwares maliciosos e violação de dados pessoais, sensíveis e/ou sigilosos.

Parágrafo único. Quaisquer dados pessoais utilizados, tratados ou compartilhados, devem seguir estritamente as diretrizes contidas na Lei Geral de Proteção de Dados nº 13709/18, bem como nas normas internas de proteção de dados do município.

CAPÍTULO IV

USO DA INTERNET E INTRANET

Art. 9º A intranet é uma rede interna de trabalho utilizada pelos servidores, sendo necessária a navegação consciente e estritamente profissional, levando em consideração as diretrizes e regras de uso.

§ 1º É vedado o uso de proxy ou qualquer outro método para burlar os mecanismos de segurança definidos pela SUBTIMA.

§ 2º O acesso aos sistemas corporativos deve ser feito exclusivamente pela rede corporativa, visando a segurança na navegação pela intranet.

§ 3º O tráfego da Internet será filtrado e bloqueado caso contenha conteúdo não autorizado.

§ 4º Se for detectada a tentativa de ligação indevida entre a internet e a rede corporativa, a estação será desconectada e o caso poderá ser comunicado à Comissão de Permanente de Proteção de Dados (CPPD).

§ 5º A SUBTIMA monitorará todos os acessos à Internet, incluindo o endereço IP e os sites acessados.

CAPÍTULO V

CONTROLE DE SOFTWARES MALICIOSOS

Art. 10. São considerados softwares maliciosos qualquer programa que prejudique ou danifique os recursos da PMDC, como vírus, worms, cavalos de troia, spyware, entre outros.

Art. 11. É vedado desabilitar ou remover softwares de segurança, como antivírus, sem a autorização da SUBTIMA.

§ 1º A SUBTIMA bloqueará o download, instalação e execução de softwares maliciosos.

§ 2º A SUBTIMA pode realizar o bloqueio manual ou de forma automática de sites que representem risco à segurança.

CAPÍTULO VI

USO DE DISPOSITIVOS MÓVEIS

Art. 12. Fica restrita a conexão de dispositivos móveis à rede corporativa, sendo de uso exclusivo dos servidores e funcionários.

Parágrafo único. Os usuários poderão ser responsabilizados por quaisquer utilizações indevidas de seus dispositivos móveis que resultem em contaminação e violação da rede corporativa.

CAPÍTULO VII

SEGURANÇA E INFRAESTRUTURA DE REDE

Art. 13. A infraestrutura de rede da PMDC, considerado de acesso restrito, inclui equipamentos de processamento, transmissão e armazenamento.

Parágrafo único. A SUBTIMA é responsável por garantir a estrutura e a segurança de rede necessária, orientando os usuários e criando novas metodologias a partir de ferramentas tecnológicas para o bom funcionamento dos setores de trabalho.

Art. 14. Durante eventos na PMDC, o acesso à Internet será permitido ao público, com acesso via rede wireless, sendo garantido pela SUBTIMA a segurança de rede e das estações de trabalho corporativas.

Parágrafo único. As informações e dados que circulam na rede corporativa são confidenciais e não devem ser capturados irregularmente e compartilhados com terceiros, devendo os casos de violações serem comunicados à CPPD.

Art. 15. Deverá a SUBTIMA garantir o suporte necessário para quaisquer incidentes na infraestrutura de rede, contando com a cooperação dos Gestores das Pastas para que os mesmos sejam solucionados com a devida urgência, e, quando for o caso, solicitar auxílio da CPPD.

CAPÍTULO VIII

USO DE IMPRESSORAS

Art. 16. As impressoras instaladas em cada setor devem ser utilizadas para fins institucionais.

§ 1º Em caso de impressoras alugadas junto a empresas terceirizadas, quaisquer chamados de manutenção deverão primeiramente ser submetidos à SUBTIMA, por setor de tecnologia da informação da Pasta pertinente, caso haja, para que os mesmos verifiquem a necessidade de comunicar às referidas empresas visando à realização de reparo.

§ 2º As impressoras próprias sofrerão diagnóstico inicial pela SUBTIMA ou pela equipe técnica de T.I. da Pasta pertinente, caso haja, onde sua manutenção poderá ser alvo de serviço contratado externamente, seguindo os trâmites legais do município para realização de serviço de terceiros.

CAPÍTULO IX

ARMAZENAMENTO

Art. 17. A SUBTIMA será responsável por disponibilizar áreas de armazenamento para os arquivos institucionais de cada setor.

§ 1º A responsabilidade pela realização de backups (cópias de segurança) dos dados armazenados, incluindo os do servidor de arquivos, é da SUBTIMA, salvo os backups de discos locais das estações de trabalho.

§ 2º As áreas de armazenamento devem ser utilizadas preferencialmente para arquivos relevantes às atividades do setor, devido à sua inviolabilidade e segurança, pois possuem a capacidade limitada, podendo ser expandidas conforme solicitação dos gestores.

§ 3º É vedado armazenamento na rede corporativa, de arquivos, softwares ou quaisquer dados e informações que não possuam objetivo profissional.

CAPÍTULO X

REDE CABEADA E CORPORATIVA

Art. 18. A rede cabeada consiste em todos os pontos de rede e telefone, incluindo qualquer conexão física, sendo a principal forma de acesso à rede corporativa.

§ 1º Apenas os dispositivos autorizados e devidamente configurados poderão ser conectados à rede cabeada, sendo proibidas as seguintes condutas:

I - Instalar ou usar qualquer equipamento que interfira, direta ou indiretamente, no funcionamento da infraestrutura de rede, como servidores DHCP, DNS, Active Directory, LDAP, entre outros;

II - Configurar IPs fixos em dispositivos conectados à rede cabeada, sem autorização;

III - Instalar Access Points, Hubs, Switches, Modems 4G, dispositivos celulares ou outros equipamentos que ampliem o acesso à rede, sem a aprovação da SUBTIMA;

IV - Realizar testes, como os de carga em sistemas ou em placas de rede, sem a anuência prévia da SUBTIMA.

§ 2º Fica estritamente proibido desconectar, alterar ou transferir conexões entre estações de trabalho e os pontos de rede, assim como entre impressoras e os pontos de rede, sem autorização prévia da SUBTIMA.

CAPÍTULO XI

MONITORAMENTO E AUDITORIA

Art. 19. As redes da PMDC, incluindo wireless, deverão ser monitoradas constantemente pela SUBTIMA.

§1º A conduta quanto aos dados trafegados entre estações de trabalho e instituições bancárias ou e-mails pessoais, ficarão a cargo servidor, inclusive quanto à utilização dos recursos tecnológicos a ele atribuídos.

§2º A SUBTIMA poderá inspecionar estações de trabalho a qualquer momento, especialmente quando houver suspeita de violação de regras, desde que haja mínima materialidade.

Art. 20. A SUBTIMA deverá manter os registros de navegação de maneira restrita, sendo fornecidos apenas em casos de avaliações por Comissões devidamente autorizadas, auditorias internas ou externas.

Parágrafo único. Não poderá ser negado nenhum dado ou registro à equipe de auditorias internas e externas, bem como à Comissão Permanente de Proteção de Dados, salvo se tal fornecimento infringir a Lei Geral de Proteção de Dados ou regulamentos internos.

CAPÍTULO XII

DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 21. Os usuários que utilizarem indevidamente os recursos tecnológicos ou violarem as diretrizes contidas nesta política, estarão sujeitos a procedimentos disciplinares definidos internamente.

Art. 22. As diretrizes e informações concernentes à privacidade no acesso às plataformas digitais do município, o que inclui cookies, serão previstas na Política de Privacidade, publicada no site Oficial do município, bem como no Portal da Transparência.

Art. 23. As regras contidas nesta política não impedem a definição de outras diretrizes de segurança da informação, através de instrução normativa, por parte das Secretarias e Procuradoria que contarem com equipe própria de tecnologia da informação, salvo se tais regras infringirem o que está estabelecido neste Decreto Municipal.

Art. 24. As unidades organizacionais, orientadas pela SUBTIMA, devem promover ações de treinamento e conscientização para que os seus colaboradores entendam suas responsabilidades e procedimentos voltados à segurança da informação.

Parágrafo único. A conscientização, a capacitação e a sensibilização em segurança da informação devem ser adequadas aos papéis e responsabilidades dos colaboradores.

Art. 25. Esta Política estará sujeita à revisão sempre que houver necessidade, visando refletir as mudanças no ambiente interno, nos riscos à segurança da informação e nas melhores práticas.

Art. 26. Este Decreto entra em vigor na data de sua publicação.

Prefeitura Municipal de Duque de Caxias, 18 de dezembro de 2024.

WILSON MIGUEL DOS REIS

Prefeito Municipal

Wilson Miguel dos Reis
Prefeito
Mat. 39529-3