DECRETO N.º 4.828 DE 01 DE FEVEREIRO DE 2017.

Redefine a Política de Informática e Segurança da Informação da Prefeitura Municipal de Miguel Pereira e dá outras providências.

O PREFEITO MUNICIPAL DE MIGUEL PEREIRA, no uso de suas atribuições que a legislação lhe confere e,

CONSIDERANDO a necessidade de aprimoramento contínuo do gerenciamento da Segurança de Informação no âmbito do Poder Executivo Municipal;

CONSIDERANDO que, os dados armazenados e gerenciados pelos Órgãos, Secretarias e Setores da Prefeitura Municipal de Miguel Pereira, devem ser controlados para garantir a sua integridade e autenticidade, evitando-se acesso e uso inadequado dos mesmos;

CONSIDERANDO que deve ser definida as responsabilidades dos envolvidos na definição dos processos suportados por sistemas de informações e projetos de TIC;

DECRETA:

Art. 1º - Fica redefinida a Política de Informática e Segurança da Informação da Prefeitura Municipal de Miguel Pereira, com as seguintes finalidades:

I – reduz custos de ocorrência de perdas e alterações indevidas de dados, preservando a confidencialidade, a integridade e a disponibilidade das informações disponíveis nos diferentes órgãos da Administração Municipal;

II - definir os critérios a serem adotados para que as informações mantenham o nível de segurança adequado à sua relevância e criticidade;

III – estabelecer preceitos, regras e modelos de segurança que possibilitem a disponibilização e utilização seguras dos serviços informatizados.

Art. 2º - A Política de Informática e Segurança da Informação redefinida por este Decreto adotará os seguintes princípios:

I – o acesso, o processamento e a disseminação de informações pela Prefeitura Municipal de Miguel Pereira através de suas redes de computadores ou de seus equipamentos isolados estará a serviço do cidadão e da sociedade, respeitando sempre os critérios de:

a) Garantia dos direitos individuais e coletivos;
b) Garantia da privacidade e segurança das pessoas físicas e jurídicas; e
c) Garantia de acessos à informações disseminadas pela Prefeitura através de seus serviços de redes.

II – A Política de Informática e Segurança da Informação da PMMP promoverá a adoção de medidas para evitar o comprometimento da integridade, confidencialidade e disponibilidade das informações durante seu manuseio, processamento, armazenamento, transporte e descarte;

III – Obrigatoriedade de elaboração de planos de contingência e de continuidade de negócios, de forma a garantir a continuidade dos serviços informatizados em caso de sinistros, desastres naturais, panes elétricas, ou quaisquer outras causas de descontinuidade.

Art. 3º - A Divisão de Informática da PMMP passa a estar subordinada à Secretaria Municipal de Administração e Recursos Humanos do Município.

CAPÍTULO I
DOS RECURSOS COMPUTACIONAIS

Art. 4º - Consideram-se recursos computacionais da rede corporativa da PMMP:

I – os hardwares e periféricos;
II – os softwares;
III – os canais de comunicação de dados, de uso exclusivo, que interligam a PMMP a outros servidores (hardware);
IV – os serviços de correio eletrônico e acesso à internet;
V – os bancos de dados.

§1º - A Divisão de Informática é a responsável pela gestão dos recursos computacionais.

§2º - Os pedidos para utilização dos recursos computacionais da rede corporativa da PMMP pelos Órgãos e Secretarias serão analisados individualmente pela Divisão de Informática.

Art. 5º - Os recursos computacionais disponíveis no âmbito da rede corporativa terá por finalidade as atividades precípuas da PMMP, sendo propriedade desta Prefeitura, não devendo ser utilizados para outro fim.

Parágrafo único – Será proibida a manutenção de equipamentos de informática pertencentes a particulares, por técnicos da Divisão de Informática nas dependências da PMMP ou às custas da PMMP.

Art. 6º - A Política de Informática e Segurança da Informação da PMMP apoia-se em procedimentos específicos fixados neste Decreto e terá por objetivo racionalizar a utilização eficiente e segura dos recurso e serviços da tecnologia da informação.

Parágrafo único – Para implementação da Política de Informática e Segurança da Informação da PMMP, a Divisão de Informática seguirá, além das normas, procedimentos e outras informações descritas neste Decreto.

CAPÍTULO II
DA IDENTIFICAÇÃO DO USUÁRIO E SENHA DE ACESSO

Art. 7º - Para utilização inicial dos recursos computacionais da rede corporativa da PMMP será necessária a abertura de ordem de serviço, com a solicitação de inscrição do funcionário no cadastro de usuários da rede corporativa da PMMP.

Art. 8º- O nome de usuário e respectiva senha serão atribuídos a um único usuário, de forma individual e intransferível, para uso exclusivo do seu titular, não devendo ser compartilhados com outros usuários.

§1º - Os usuários serão responsabilizados por todos os acessos e atividades desenvolvidas através do seu nome de usuário, inclusive por eventuais danos decorrentes de sua má utilização.

§2º - A utilização dos recursos de informática deverá ser feita de forma a preservar a segurança das informações e a inobservância ao previsto neste Decreto sujeita o responsável a sanções administrativas, sem prejuízo das cominações legais eventualmente cabíveis na área cível e criminal, excetuando-se do disposto neste parágrafo os casos de atuação institucional de usuários quando em cumprimento de determinação superior formal.

§ 3º – Incumbe a cada usuário cadastrado:

I – conhecer e seguir as diretrizes da Política de Informática e Segurança da Informação da PMMP, inclusive no tocante à sua segurança;

II – informar à Divisão de Informática qualquer suspeita ou incidência de contaminação da sua estação de trabalho;

III – realizar procedimentos prévios de segurança, após informativos a serem disponibilizados na intranet pela Divisão de Informática, a fim de evitar o recebimento de arquivos, através de qualquer mídia eletrônica que possam comprometer sua estação de trabalho;

IV – restringir o acesso à Internet preferencialmente ao desempenho de suas atividades profissionais no âmbito da Instituição;

V – manter intacta a configuração da estação de trabalho, somente procedendo a qualquer alteração com consentimento da Divisão de Informática;

VI – encerrar sua sessão de trabalho sempre que se ausentar do equipamento que estiver utilizando;

VII – desligar sua CPU ao término do seu expediente;

VIII – notificar à Divisão de Informática sobre qualquer fraude, sabotagem, desvio ou falha na segurança da informação que chegue ao seu conhecimento.

Art. 9º– Será vedada a apropriação de nome de usuário e senha de outros usuários.

Art. 10 – Os casos de mudança de lotação, afastamento e retorno de usuário deverão ser comunicados à Divisão de Informática pelo órgão responsável pela administração destes, através da abertura de ordem de serviço.

§ 1º – Os nomes de usuários que não forem utilizados por mais de 03 (três) meses serão automaticamente desabilitados.

§ 2º – No caso de afastamento publicado no BIM-MP, o nome de usuário, a conta de correio e demais permissões serão automaticamente desabilitados.

Art. 11 – As senhas, preferencialmente, deverão ser alfanuméricas e conter entre 06 (seis) e 08 (oito) caracteres.

Parágrafo Único – Recomenda-se que a senha seja substituída regularmente.

CAPÍTULO III
DO USO DOS SERVIDORES E DAS ESTAÇÕES

Art. 12– Será vedada a instalação ou desinstalação de recursos computacionais de qualquer procedência, bem como o desenvolvimento ou implantação de qualquer sistema ou aplicativo, na rede corporativa da PMMP, sem a prévia e expressa autorização da Divisão de Informática.

Parágrafo Único – A utilização, por parte de qualquer usuário da rede, de programa não autorizado ou não adquirido legalmente, caracteriza infringência à Lei Federal n.º 9.609/1998, que dispõe sobre a proteção da propriedade intelectual de programas de computador e sua comercialização no País.

Art. 13 – Será vedado instalar, manter e acessar nas estações de trabalho e nos computadores servidores arquivos com conteúdo pornográfico, erótico, discriminatório, para entretenimento, ofensivos aos direitos humanos e outros não relacionados às atividades institucionais e administrativas da PMMP (ex.: redes sociais, programas de downloads para MP3 e Filmes).

Art. 14 – Será vedado o compartilhamento de diretórios, arquivos e demais recursos computacionais sem prévia autorização da Divisão de Informática.

Parágrafo Único – A detecção de compartilhamento não autorizado, que ponha em risco a segurança da rede, implicará na desconexão imediata da estação até a apuração de responsabilidade e as providências cabíveis.

Art. 15 – Os usuários deverão zelar pela conservação, integridade, correta utilização e segurança dos recursos computacionais sob sua responsabilidade.

§ 1º – Qualquer intervenção na estação de trabalho somente poderá ser efetuada por técnico da Divisão de Informática obrigatoriamente assistido pelo usuário.

§ 2º – O serviço de mensageiro somente poderá ser utilizado para envio de mensagens pertinentes às atividades precípuas da PMMP, e que sejam de interesse de todos os servidores.

Art. 16 – O usuário deverá exigir identificação do técnico designado para atendimento de manutenção ou verificação dos recursos computacionais e a apresentação da ordem de serviço, verificando a autenticidade, se necessário, junto à chefia responsável da Divisão de Informática.

Art. 17 – A realização de backup dos dados contidos nas estações de trabalho os quais, não estiverem na rede de dados e internet da PMMP, será de responsabilidade do usuário.

Art. 18 – A realização de backup dos dados contidos nos servidores, incluindo o servidor de arquivos, será de responsabilidade da Divisão de Informática, sendo efetuado diariamente.

§ 1º – O servidor de arquivos será usado, preferencialmente, para armazenamento e manutenção de arquivos de relevância, devido às suas características de inviolabilidade e segurança, sendo disponibilizado somente aos usuários certificados e credenciados pela Divisão de Informática.

§ 2º – O backup dos dados permanecerá disponível pelo período de 180 (cento e oitenta) dias, após o que será descartado.

Art. 19 – Para diagnóstico de problemas nos recursos computacionais, inclusive em caso de suspeita de violação de regras, a Divisão de Informática poderá acessar arquivos nos servidores e estações de trabalho, com o conhecimento prévio do chefe imediato do usuário.

Art. 20 – O acesso remoto às estações de trabalho, com o objetivo de suporte e manutenção dos recursos computacionais, só poderá ser realizado por equipe autorizada da Divisão de Informática, sempre com prévia permissão do usuário ou do seu chefe imediato.

Art. 21 – Será vedado ao usuário e ao chefe imediato do usuário impedir que procedimentos técnicos realizados por pessoal autorizado pela Divisão de Informática, devidamente identificado e de posse de ordem de serviço, sejam executados nas estações de trabalho sob sua responsabilidade.

CAPÍTULO IV
DO USO DA INTRANET

Art. 22 – Considera-se intranet da PMMP todos os recursos computacionais disponíveis nos segmentos da rede corporativa, conceituados no art. 1º e seus incisos, excetuando-se o acesso à internet.

Art. 23 – Cabe à Divisão de Informática identificar e ajustar o porte dos canais de comunicação, a fim de adequá-los à demanda, bem como estabelecer e revisar periodicamente os critérios de priorização.

Art. 24 – O acesso à intranet será permitida a todos os usuários da rede corporativa da PMMP, previamente autorizados e através do nome de usuário e respectiva senha.

Art. 25 – Para a transferência de arquivos através da intranet, durante o expediente administrativo, com tamanho superior ao limite estabelecido pela Divisão de Informática, deverão ser utilizados meios transportáveis (CD, DVD, Zip disk, pen drives, etc), evitando o uso da rede interna ou dos canais de comunicação.

§ 1º – O tamanho limite para a transferência de arquivos será estabelecido pela Divisão de Informática, por meio de Orientação Técnica, podendo ser alterado conforme a evolução tecnológica.

§ 2º – As exceções poderão ser autorizadas pela Divisão de Informática, mediante solicitação por escrito, comprovada a imperiosa necessidade de serviço.

CAPÍTULO V
DO USO DA INTERNET

Art. 26 – O acesso dos usuários da rede corporativa à internet deverá ser feito exclusivamente por meio da ligação existente entre a PMMP e a rede mundial de computadores.

Art. 27 – Conexões com a intranet e internet, através de linha discada e modem, somente poderão ser adotadas nas estações não interligadas à rede corporativa da PMMP enquanto permanecerem totalmente isoladas, com expressa e prévia autorização da Divisão de Informática.

Parágrafo Único – A detecção da situação configurada no *caput* deste Artigo implicará na desconexão imediata da estação, até a apuração de responsabilidades e providências cabíveis.

Art. 28 – O acesso à internet através da rede corporativa será permitido somente aos usuários previamente autorizados, através de nome de usuário e respectiva senha, cuja concessão se dará mediante solicitação por escrito, dada pelo chefe imediato e após análise da política para liberação de acessos.

Art. 29 – Será vedado o acesso à sites da internet de conteúdo não autorizado, tais como os de conteúdo pornográfico, erótico, músicas, jogos, vídeos, sites ofensivos aos direitos humanos e salas de bate-papo (chats), rádios on-line, bem como recursos do tipo FTP, ICQ e programas de cópia de arquivos (download) ponto a ponto (Ex.: Emule, Kazaa, Gnutella, Imesh, Morpheus, etc), Torrent e P2P.

§ 1º – Comprovada a imperiosa necessidade de serviço o acesso poderá ser autorizado pela Divisão de Informática, mediante solicitação por escrito dada pelo chefe imediato do órgão no qual o usuário está lotado.

§ 2º – A lista completa, com eventuais alterações nas políticas de acesso aos sítios e serviços, será disponibilizada a todos os usuários através da intranet.

Art. 30 – A execução de cópia de arquivo via internet será passível de priorização durante o expediente administrativo, de modo a não concorrer com as atividades precípuas da PMMP.

Art. 31 – Os acessos à internet são passíveis de monitoração e identificação quanto ao nome de usuário, endereço da máquina do usuário e site acessado, visando à identificação de possível infração às vedações impostas.

Art. 32 – Não será permitido mais de um acesso simultâneo à internet com um mesmo nome de usuário e, no caso de sua detecção, o nome de usuário e respectiva senha serão desativados, sendo a reativação do nome de usuário condicionada à abertura de uma ordem de serviço, com a liberação de acesso à internet analisada mediante solicitação por escrito do usuário.

CAPÍTULO VI
DO USO DO CORREIO ELETRÔNICO

Art. 33 – A caixa postal de correio eletrônico, que poderá ser individual ou institucional, será disponibilizada pela Divisão de Informática somente aos usuários ou órgãos previamente autorizados, cuja concessão se dará mediante solicitação por escrito dada pelo chefe imediato e após análise da política para liberação de acessos.

Art. 34 – As caixas postais do correio eletrônico institucional são de propriedade da PMMP, passíveis de monitoração pela Divisão de Informática em caso de fragilidades ou ameaças, ocorridas ou suspeitas, na segurança de sistemas ou serviços, com o conhecimento prévio do chefe imediato e autorização da Comissão de Normatização Computacional da PMMP.

Art. 35 – Será vedado manter, enviar, replicar ou encaminhar mensagens, por meio do correio eletrônico institucional, com conteúdo não relacionado às atividades precípuas da PMMP.

§ 1º – O usuário deverá excluir da caixa postal institucional qualquer mensagem recebida estranha às atividades precípuas da PMMP, tão logo identificado o conteúdo inadequado.

§ 2º – Só será permitido o uso do correio eletrônico institucional para veiculação de campanhas internas, de caráter social, mensagens informativas ou outras que eventualmente possam ter conteúdo vedado, mediante autorização da Comissão de Normatização Computacional da PMMP.

Art. 36 – O tamanho da caixa postal de correio eletrônico será limitado para todos os usuários da rede corporativa da PMMP, de acordo com a necessidade de interação das atividades do órgão.

§ 1º – As caixas postais que excederem ao limite estabelecido pela Divisão de Informática receberão mensagens de alerta do administrador de correio e ficarão automaticamente impossibilitadas de enviar e receber mensagens.

§ 2º – Será responsabilidade do usuário a manutenção da sua caixa postal, eliminando ou transferindo para pastas particulares as suas mensagens recebidas ou enviadas há mais de 90 (noventa) dias e suas mensagens excluídas há mais de 30 (trinta) dias.

Art. 37 – O tamanho máximo dos arquivos anexados às caixas postais fica limitado pela Divisão de Informática, por meio de Orientação Técnica, sendo a liberação de arquivos recebidos que excedam ao limite estabelecido autorizada pela Divisão de Informática, mediante solicitação por escrito, desde que comprovada a imperiosa necessidade de serviço.

Art. 38 – Os arquivos anexados em mensagens recebidas serão bloqueados, caso sejam arquivos que potencialmente possam conter programas maliciosos, sendo a lista de tipos de arquivos bloqueados passível de consulta na página da Intranet da PMMP.

Parágrafo Único – O usuário deverá solicitar o desbloqueio através da abertura de ordem de serviço, caso necessite receber mensagens através do correio eletrônico, com arquivo anexado descrito no *caput* deste artigo, devendo a Divisão de Informática providenciar a verificação do arquivo e seu encaminhamento, no caso de inexistência de vírus.

Art. 39 – O recebimento de mensagens será filtrado para bloqueio de mensagens geralmente com finalidades comerciais (spam), mensagens contendo boatos maliciosos (hoaxe) e outros tipos de mensagens indesejáveis.

Art. 40 – Recomenda-se não abrir mensagens de remetente ou conteúdo suspeito. Em caso de dúvida, solicite suporte à Divisão de Informática, através da abertura de ordem de serviço.

CAPÍTULO VII
DO CONTROLE DOS PROGRAMAS MALICIOSOS

Art. 41 – São considerados programas maliciosos: vírus, vermes (worms), cavalos de tróia (trojan horses), programas espiões (spywares), programas de invasão e todos aqueles que possam prejudicar ou danificar os recursos computacionais e tornar vulneráveis as informações corporativas da PMMP.

Art. 42 – Será vedado remover ou desabilitar programas de controle e remoção de programas maliciosos licenciados para a rede corporativa, bem como instalar qualquer outro não licenciado pela PMMP.

CAPÍTULO VIII
DO USO DE COMPUTADORES MÓVEIS

Art. 43 – Consideram-se computadores móveis equipamentos tais como: notebooks, palmtops, laptops e telefones celulares (smartphones).

Art. 44 – Será vedada a conexão de computadores móveis à rede corporativa da PMMP sem a prévia verificação contra programas maliciosos e sem a adequada atualização do programa antivírus e do sistema operacional.

Parágrafo Único – A Divisão de Informática prestará o suporte necessário para tal desinfecção e atualização, através da abertura de ordem de serviço.

Art. 45 – A verificação de programas maliciosos, atualização do antivírus e sistema operacional deverá ser observada também fora da rede da PMMP, com o objetivo de evitar o acesso não autorizado e a divulgação de informações armazenadas nos computadores móveis.

Parágrafo Único – Por se tratarem de equipamentos facilmente transportáveis, é importante que cuidados especiais sejam tomados, com o objetivo de evitar a exposição ou furto de informação.

CAPÍTULO IX
DO USO, AQUISIÇÃO E INSTALAÇÃO DE PROGRAMAS DE COMPUTADORES.

Art. 46 – As Secretarias, órgãos e setores do Poder Executivo Municipal utilizarão, preferencialmente, programas de computador com código aberto, isentos de reservas de direitos proprietários quanto às condições de seu uso, modificação, customização, cessão, liberdade de instalação, plena utilização, acesso ao código fonte, distribuição, padronização e, fundamentalmente, sem ônus de aquisição de licenças.

Parágrafo Único – A migração do uso de programas proprietários para outros similares de código aberto deverá basear-se em estudos técnicos preliminares que definam um cronograma criterioso e que assegurem a qualidade e eficiência dos correspondentes serviços.

Art. 47 – A aquisição de programas proprietários, com ou sem instalação à aquisição de máquinas, deverá observar o seguinte:

I – análise da destinação do uso do equipamento e do programa, de modo a se considerar a possibilidade técnica de plena utilização de solução não proprietária;

II – parecer técnico circunstanciado atestando a inexistência de programas com código aberto que possa atender, restritivamente, as exatas funcionalidades necessárias para as áreas usuárias;

III – preferência para produtos que operem em ambiente multiplataforma para uso, sem restrições, sob sistemas operacionais de código livre.

Parágrafo Único – Preferências de ordem estéticas e subjetivas ou a existência de funcionalidades maiores, porém desnecessárias ao serviço público, não deverão ser consideradas na avaliação de compra de programas proprietários.

Art. 48– A Divisão de Informática da Secretaria Municipal de Administração e Recursos Humanos deverá no prazo de 90 (noventa) dias, elaborar estudo de viabilidade técnica para migração das suas atuais soluções proprietárias para alternativas com código aberto, respeitando-se o seguinte:

I – planejamento, a longo prazo, para migração de soluções que não permitam, imediatamente e sem prejuízo para os serviços, a adoção de alternativas sem ônus com a renovação de licenças ou aquisições de novas licenças;

II – avaliação de uso de estações de trabalho em plataforma de código aberto que garantam eficiência para os serviços, e que não dependam da integração com outros aplicativos proprietários.

Art. 49 – Fica definido como padrão de uso dos órgãos do Poder Executivo Municipal a suíte de escritório "Libre Office", respeitando-se o dispositivo no art. 48, I e II, deste Decreto.

CAPÍTULO IX
DISPOSIÇÕES FINAIS

Art. 50 – Os usuários deverão notificar seus superiores ou à Divisão de Informática sobre quaisquer fragilidades ou ameaças, ocorridas ou suspeitas, na segurança dos sistemas, serviços ou informações, mesmo que estes não estejam diretamente sob sua responsabilidade.

§ 1º – Para sua própria proteção, em nenhuma hipótese deverá ser feita uma averiguação de fragilidade por conta própria, sendo essa investigação interpretada como potencial uso impróprio do sistema.

§ 2º – Todos os limites e políticas referidos neste ato (arts. 24, 27, 28, 32, 36, 37 e 38) ficarão disponíveis na página da Divisão de Informática na intranet e serão passíveis de atualização, devendo ser consultados periodicamente ou sempre que houver dúvida quanto à sua aplicação.

Art. 51 – Os casos de desrespeito às normas estabelecidas neste Decreto serão encaminhados pela Divisão de Informática à Secretaria Municipal de Administração e Recursos Humanos para a adoção das providências cabíveis, nos termos da legislação vigente.

Art. 52 – As solicitações deverão ser encaminhadas à Divisão de Informática, por Comunicação Interna (CI), com justificativa adequada, quando se tratar de:

a) criação de caixa de correio;

b) ampliação de limite superior ao estabelecido;

c) autorização de acesso;

d) autorização para transferências de arquivos;

e) auditoria de segurança;

f) análise ou informação quanto ao uso indevido dos recursos computacionais.

Art. 53 – A Secretaria Municipal de Administração e Recursos Humanos, por meio de Resoluções específicas do Secretário Municipal de Administração e Recursos Humanos, regulamentará normas de segurança complementares a Política de Informática e Segurança da Informação da PMMP, após apreciação e aprovação da Comissão de Normatização Computacional da PMMP.

Art. 54 – A Secretaria Municipal de Administração e Recursos Humanos fará exames periódicos a fim de avaliar o cumprimento da Política de Informática e Segurança da Informação da PMMP, assim como de suas normas de segurança complementares.

Art. 55 – Este Decreto entrará em vigor na data da sua publicação, revogadas as disposições em contrário, em especial o Decreto Municipal n.º 3.401, de 28 de outubro de 2008.

Prefeitura Municipal de Miguel Pereira,
Em, 01 de fevereiro de 2017.

ANDRÉ PINTO DE AFONSECA
- Prefeito Municipal-

PREFEITURA MUNICIPAL DE
MIGUEL PEREIRA
EST. DO RIO

Publicado em 01a10/02/2017
BOLETIM INFORMATIVO DO MUNICÍPIO DE MIGUEL PEREIRA
Página 02a04 Bim nº 410
Rúbrica
Mat. 01/2450