DECRETO Nº 339, DE 24 DE ABRIL DE 2018.

PUBLICADO NO QUADRO DE AVISO DA PREFEITURA MUNICIPAL DE PARAUAPEBAS EM: 24 / 04 / 2018

DISPÕE SOBRE PROCEDIMENTOS PARA SEGURANÇA FÍSICA E LÓGICA DOS EQUIPAMENTOS, SISTEMAS, DADOS E INFORMAÇÕES DA PREFEITURA MUNICIPAL DE PARAUAPEBAS.

O PREFEITO MUNICIPAL DE PARAUAPEBAS, no uso das atribuições que lhe são conferidas por Lei, em especial as emanadas da Lei Orgânica Municipal,

RESOLVE:

CAPÍTULO I – DA FINALIDADE

Art. 1° O presente Decreto dispõe sobre os procedimentos para segurança física e lógica dos equipamentos, sistemas, dados e informações, objetivando a implementação de rotinas de trabalho, procedimentos de controle, melhoria das condições gerais de segurança de toda a rede da Prefeitura e otimização dos resultados do trabalho.

CAPÍTULO II – DA ABRANGÊNCIA

Art. 2° Todas as unidades da estrutura administrativa do Município, no âmbito da operacionalização dos procedimentos do sistema de tecnologia da informação estão abrangidos por esta regulamentação e, ainda, todos os usuários de recursos de tecnologia da informação, executores de tarefas, fornecedores ou recebedores de dados e informações em meio documental ou informatizado, que deverão observar a legislação municipal, estadual, federal e os procedimentos constantes deste Decreto.

CAPÍTULO III– DOS CONCEITOS

Art. 3° Para os fins deste Decreto considera-se:

I - manual de rotinas internas e procedimentos de controle: coletânea de instruções normativas que tem por objetivo veicular as informações necessárias à execução das atividades;

II - recursos tecnológicos: os equipamentos, as instalações e bancos de dados direta e indiretamente administrados, mantidos ou operados pelas diversas secretarias, órgãos, diretorias, coordenadorias e gerências, tais como:

a) computadores (desktop ou notebook), incluídos seus equipamentos: CD's/DVD's, pendrive e acessórios;
b) impressoras, plotters e equipamentos multifuncionais conectados ao computador;
c) redes de computadores e de transmissão de dados;
d) bancos de dados ou documentos residentes em disco, fita magnética ou outros meios;
e) leitores de códigos de barra, scanners, equipamentos digitalizadores e afins.
f) Manuais técnicos e CD's/DVD's de instalação/configuração;
g) patch panel, switches, hubs, appliance e outros ativos de rede;
h) serviços e informações disponibilizados via arquitetura de informática da instituição;
i) softwares, sistemas e programas adquiridos ou desenvolvidos pela Administração.

III - usuário interno: todo servidor público municipal que utilize algum recurso de tecnologia da informação municipal;

IV - usuário externo: prestador de serviço ou população em geral quando em uso da rede pública;

V - cadastro: procedimento de criação de usuário para acesso aos sistemas informatizados da Prefeitura Municipal;

VI - habilitação: procedimento de atribuição dos módulos ao usuário;

VII - módulo: subconjunto de transações de um sistema, que define a abrangência de atuação de um usuário;

VIII - senha: conjunto alfanumérico de caracteres destinado a assegurar a identidade do usuário de permitir seu acesso aos dados, programas e sistemas não disponíveis ao público, de uso pessoal e intransferível;

IX - ativos de informação: o patrimônio composto por todos os dados e informações gerados e manipulados nos processos do órgão;

X - ativos de processamento: patrimônio composto por todos os elementos de hardware (máquina), software (sistema) e infraestrutura de comunicação, necessários para a execução das atividades do órgão;

XI - recursos de tecnologia da informação: conjunto dos ativos de informação e de processamento;

XII - dado: qualquer elemento identificado em sua forma bruta que por si só não conduz a uma compreensão de determinado fato ou situação, constituindo um insumo de um sistema de informação;

XIII - informação: resultado do processamento do conjunto de dados apresentados a quem de direito, na forma, tempo e meio adequado, que permite conhecer uma avaliação ou fato, contribuindo para a tomada de decisão;

XIV - informações íntegras: aquelas que, apenas são alteradas através de ações autorizada e planejadas;

XV - informações integradas: aquelas que fazem parte de um todo que se completam ou complementam;

XVI - sistema de informação: conjunto de partes que formam um todo unitário, com o objetivo de disciplinar informações para formular, atingir e avaliar as metas da organização;

XVII - tecnologia da informação: conjunto de equipamentos e suportes lógicos que visam coletar, processar, tratar, armazenar e distribuir dados e informações;

XVIII - confidencialidade: o princípio de segurança que trata da garantia de que o acesso à informação seja obtido somente por pessoas previamente autorizadas;

XIX - integridade: o princípio de segurança que trata da salvaguarda da exatidão e confiabilidade da informação e dos métodos de processamento;

XX - disponibilidade: o princípio de segurança que trata da garantia de que pessoas autorizadas obtenham acesso à informação e aos recursos correspondentes, sempre que necessário;

XXI - segurança da informação: a preservação da confidencialidade, integridade, credibilidade e disponibilidade da informação, adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade podem estar envolvidas;

XXII - credencial: a combinação do "login" e "senha", utilizado ou não em conjunto a outro mecanismo de autenticação que visa legitimar e conferir autenticidade ao usuário na utilização de infraestrutura e recursos de informática;

XXIII - suporte técnico: serviço realizado pela equipe dos setores de informática que tem a responsabilidade de dar suporte aos usuários.

CAPÍTULO IV – DAS RESPONSABILIDADES

Art. 5° São responsabilidades da Secretaria Municipal de Planejamento e Gestão (SEPLAN), enquanto unidade responsável pela execução deste Decreto:

I - promover discussões técnicas com os diversos setores da Prefeitura, para auxiliar na definição das rotinas de trabalho, identificação dos pontos de controle,

organizar a demanda de qualificação e formação de servidores, coordenar a elaboração e execução de convênios e ações com outras instituições públicas e privadas, no âmbito deste Decreto;

II - promover o nivelamento de conhecimento e a integração dos diversos setores da tecnologia da informação, por meio da realização de cursos de capacitação, instrumentos de formação e informação que pedagogicamente auxiliem na introdução de novo programas e sistemas, que otimizem o trabalho dos servidores que atuam dentro da Prefeitura;

III - realizar a promoção e divulgação deste Decreto, auxiliando os demais departamentos da Prefeitura na sua adoção;

IV - manter atualizada, orientar as áreas executoras e supervisionar a aplicação deste Decreto;

V - potencializar o uso da informação e da tecnologia da informação no cumprimento da missão do município;

VI - subsidiar com informações necessárias e suficientes o processo de tomada de decisão da Administração Pública;

VII - disponibilizar informações que possibilitem à Administração Pública o atendimento das necessidades do cidadão;

VIII - possibilitar qualidade e transparência às ações de governo permitindo um melhor controle social;

IX - promover a evolução, de forma coordenada, dos assuntos relacionados à informação e tecnologia da informação no âmbito da Administração Pública Municipal, visando a melhoria do desempenho das pessoas nos processos da organização;

X - promover a sinergia das ações da Administração Pública no intuito de propiciar a inclusão digital;

XI - promover o livre intercâmbio de informações e conhecimentos com a sociedade, contribuindo para o seu desenvolvimento;

XII - propiciar a melhoria da gestão pública, contribuindo para a produção de resultados que promovam a justiça social;

XIII - coordenar no âmbito do Governo as ações do governo eletrônico;

XIV - analisar periodicamente a efetividade da política de segurança da informação, propondo mecanismos institucionais para melhoria contínua bem como assessorar, em matérias correlatas, nas demais unidades da Administração Municipal;

XV - avaliar as mudanças importantes na exposição dos recursos a riscos, identificando as principais ameaças;

XVI - analisar criticamente os incidentes de segurança da informação e ações corretivas correlatas.

XVII - promover o aprimoramento dos procedimentos de controle e o aumento da eficiência operacional;

XVIII - manter este Decreto à disposição de todos os funcionários da Prefeitura, visando seu fiel cumprimento;

XIX - cumprir fielmente as determinações em especial quanto aos procedimentos de controle e quanto à padronização dos procedimentos na geração de documentos, dados e informações;

XX - conscientizar os usuários internos e colaboradores sob sua supervisão em relação aos conceitos e as práticas de segurança da informação;

XXI - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à segurança da informação;

XXII - comunicar ao superior imediato e a unidade competente em caso de comprometimento da segurança e quaisquer outras faltas, desvios ou violação das regras estabelecidas para adoção de medidas cabíveis;

XXIII - disponibilizar softwares de interesse da administração pública;

XXIV - participar da elaboração e implantação de todo e qualquer software que seja inserido ao parque computacional e/ou disponibilizado aos usuários do serviço público;

XXV - disponibilizar a todos os outros setores de tecnologia da informação, uma versão livre de código aberto, do sistema operacional oficial adotado pela Prefeitura;

XXVI - estabelecer quais são os softwares de tipo OFFICER e sistema operacional, que serão utilizados pela Prefeitura;

XXVII - capacitar e auxiliar os usuários durante a adaptação a novos softwares usados pela rede municipal;

XXVIII - através da atividade de auditoria interna, avaliar a eficiência dos procedimentos de controle inerentes a cada sistema administrativo, propondo alterações no decreto para aprimoramento dos controles ou mesmo a formatação de novos decretos;

XXIX - reportar aos responsáveis sobre as quebras de segurança, caso ocorram;

XXX - organizar e manter atualizado o manual de procedimentos;

XXXI - prover ou assessorar a contratação de recursos de tecnologia da informação, inclusive ampliação e manutenção dos sistemas.

Art. 6º São responsabilidades da Secretaria Municipal de Obras e da Secretaria Municipal de Serviços Urbanos:

I - adotar em qualquer projeto de construção ou reforma, previsão de rede de computadores de acordo com as normas ABNT NBR 16415, ABNT NBR 14565, e demais normas aplicáveis;

II – adotar em qualquer projeto de construção ou reforma a previsão de sistemas de aterramentos de acordo com as normas técnicas aplicáveis.

CAPÍTULO V – DOS PROCEDIMENTOS

Seção I – Das obrigações e permissões dos usuários

Art. 7º A política de segurança da informática se aplica a todos aqueles que exerçam, por nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, cargo, emprego ou função pública no âmbito da Administração Municipal e que façam uso de seus recursos materiais e tecnológicos.

Art. 8º A fim de resguardar a continuidade, integridade, credibilidade e disponibilidade das informações e serviços devem ser adotados mecanismos de proteção.

Art. 9º Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela Prefeitura Municipal é considerada de sua propriedade e deve ser protegida, de acordo com este Decreto.

Art. 10. Deverão ser realizadas auditorias periódicas dos ativos, de forma a aferir o correto cumprimento da política de segurança da informação.

Art. 11. Fica assegurado ao suporte técnico, de ofício ou a requerimento do responsável pela unidade administrativa, necessariamente referendado pelo secretário da pasta, a qualquer tempo, a competência de suspender temporariamente o acesso do usuário à recurso de tecnologia da informação da Prefeitura, quando evidenciados riscos à segurança da informação.

Art. 12. Caberá à SEPLAN elaborar, revisar, atualizar, divulgar e validar as diretrizes, normas, procedimentos e instruções, que regulamentam os princípios e valores existentes na política de segurança da informação, visando à regulamentação e operacionalização das diretrizes apresentadas neste Decreto.

Art. 13. As normas e procedimentos deverão ser elaboradas tomando-se por base os objetivos e controles estabelecidos na ABNT NBR ISO/IEC 17799 e na Lei Federal nº 12.527 de 18 de novembro de 2011, quais sejam:

I - organização da segurança da informação;

II - gestão de ativos;

III - segurança em recursos humanos;

IV - segurança física e do ambiente;

V - gerenciamento das operações e comunicações;

VI - controles de acessos;

VII - aquisição, desenvolvimento e manutenção de sistemas de informação;

VIII - gestão de incidentes de segurança da informação;

IX - gestão da continuidade do negócio;

X – conformidade;

XI - divulgação de informação de interesse público.

Art. 14. Todos os recursos de tecnologia da informação da Prefeitura devem ser inventariados, classificados, atualizados periodicamente e mantidos em condição de uso.

Art. 15. Deverá ser implementado processo de gerenciamento de riscos, visando a identificação e mitigação dos mesmos, associados às atividades críticas da Prefeitura.

Art. 16. Deverão ser elaborados planos de continuidade de negócio para cada atividade crítica de forma a garantir o fluxo das informações necessárias em momento de crise e o retorno seguro à situação de normalidade.

Seção II – Das contas de acesso

Art. 17. Para utilizar os computadores e obter acesso ao correio eletrônico, internet da rede corporativa do Município, software, aplicativos e pastas em geral, o departamento pessoal deverá enviar memorando endereçado a SEPLAN solicitando abertura de conta de acesso (login) e senha para o servidor, na investidura do cargo.

Art. 18. Em virtude de rompimento de vínculo institucional entre o servidor e a Prefeitura, o departamento pessoal deverá solicitar imediatamente o bloqueio de acesso.

Art. 19. As contas de acesso aos recursos de tecnologia de informação terão a seguinte padronização:

I - e-mail institucional pessoal: (primeiro nome) (último sobrenome)@parauapebas.pa.gov.br;

II - e-mail institucional de gerência, coordenadoria, diretoria, assessoria e secretaria: (nome do órgão)@parauapebas.pa.gov.br.

Art. 20. O e-mail institucional gerencial será utilizado pelo superior responsável da respectiva gerência ou a quem por ele for designado, por escrito, para fins de comunicação com outros órgãos e entidades, com o objetivo de centralizar as informações estratégias do órgão em um único e-mail.

Art. 21. O departamento pessoal deverá encaminhar a lista com os dados dos servidores, classificados por órgão de lotação, que necessitem utilizar contas de e-mail institucional.

Art. 22. Ao receber a conta de acesso, o usuário ou colaborador deverá assinar e cientificar o termo de responsabilidade de utilização de recursos de tecnologia da informação da Prefeitura, disponibilizado pela SEPLAN.

Art. 23. Mudança de lotação, atribuições, afastamento definitivo ou temporário do usuário, deverá automaticamente ser comunicado a SEPLAN pelo departamento de pessoal, para os procedimentos de ajustes ou cancelamento de conta de acesso, cabendo a este departamento o ônus por qualquer uso indevido da credencial do usuário decorrente da não comunicação de algum dos eventos tratados neste item.

Art. 24. Os usuários deverão manter os equipamentos nas suas perfeitas condições de uso na forma como lhes foram entregues, evitando a colagem de adesivos ou outros enfeites particulares.

Art. 25. Os usuários não deverão colocar objetos sobre os equipamentos de forma a prejudicar o seu sistema de ventilação, assim como manipular líquidos, alimentos ou substâncias que possam ocasionar danos quando os estiver operando.

Art. 26. O usuário deverá encerrar sua sessão (desligar ou fazer logoff) na estação de trabalho ao término de suas atividades, sendo que, ao final do expediente a estação de trabalho deverá ser desligada.

Art. 27. Os usuários devem alterar suas senhas iniciais no primeiro acesso, sendo responsáveis por todas as ações realizadas mediante os logins e senhas que lhe são atribuídos.

Seção III – Dos softwares e hardwares

Art. 28. Todo software existente no parque computacional da Prefeitura deverá ser classificado como Open Source (software de uso livre), ou software proprietário, desde que a obrigatoriedade do uso esteja devidamente justificada, referendada pelo secretário da pasta e o software esteja licenciado.

Art. 29. Toda instalação de software deverá ser realizada pela equipe de suporte técnico.

Art. 30. É proibida a transferência de qualquer tipo de programa, jogo, e similares, para a rede interna da Prefeitura.

Art. 31. É proibido o uso de jogos, inclusive os da internet (online);

Art. 32. É vedada a abertura de computadores, para qualquer tipo de reparo, o que deve ser feito através solicitação ao setor competente por telefone ou memorando.

Art. 33. Não é permitida a alteração das configurações de rede.

Art. 34. Todo software instalado nos computadores, por padrão, é de posse da instituição, sendo vedada a cópia, clone, uso de licença ou qualquer outra forma de disponibilizá-los a terceiros.

Art. 35. Não é permitido ao usuário a remoção dos softwares padrão instalados nos computadores.

Art. 36. Não é permitido ao usuário a instalação de softwares em equipamentos de propriedade da Prefeitura Municipal de Parauapebas.

Seção IV – Do ambiente de rede

Art. 37. O suporte técnico da SEPLAN disponibilizará os pontos de rede necessários ao desenvolvimento das atividades de cada órgão. Qualquer alteração ou criação de um ponto novo deverá ser comunicado num tempo hábil, bem como o fornecimento do material necessário à execução do serviço.

Art. 38. É expressamente proibido o uso de meios ilícitos de acesso aos computadores, sistemas e arquivos do ambiente de rede computacional municipal.

Art. 39. É proibido o acesso remoto aos computadores da rede pública municipal sem o conhecimento ou consentimento do usuário.

Art. 40. Não deverão ser utilizados quaisquer materiais ou informações, incluindo arquivos, textos, planilhas ou imagens disponiveis na rede corporativa do Município, que não respeitem os direitos autorais, marcas registradas, patentes, sigilos comerciais ou outros direitos de propriedade intelectual de terceiros.

Art. 41. Fica proibido tentar burlar a utilização dos recursos computacionais do Município com o objetivo de obter proveito pessoal ou violar sistemas de segurança estabelecidos.

Art. 42. Na rede corporativa da Prefeitura fica expressamente proibido:

I – o uso de dispositivos móveis pessoais (celulares/tablets/notebooks), salvo em casos estritamente necessários e devidamente autorizados;

II - a instalação e configuração de equipamentos de rede pessoais.

Seção V – Do correio eletrônico (e-mail)

Art. 43. O acesso ao sistema de correio eletrônico será disponibilizado aos usuários com necessidade manifesta de usá-lo como ferramenta de apoio às atividades profissionais.

Art. 44. Não será permitido participar, criar, ou distribuir voluntariamente mensagens indesejáveis, como circulares, manifestos públicos, correntes de cartas, SPAM ou similares que possam prejudicar o trabalho de terceiros, causar tráfego na rede ou sobrecarregar os sistemas computacionais desnecessariamente.

Parágrafo único. Considera-se *spam* o envio em massa de e-mails para usuários que não os solicitaram de forma explícita e com os quais o remetente não mantenha qualquer vínculo de relacionamento profissional e cuja quantidade comprometa o bom funcionamento dos servidores de e-mail.

Art. 45. Não é permitido o uso de endereços de e-mail para trocas de informações ligadas a práticas que infrinjam qualquer ordenamento jurídico legal.

Art. 46. O usuário não deverá abrir e-mail com arquivos anexados quando não conhecer o remetente sob risco de estar infectando com vírus o equipamento e a própria rede de dados.

Art. 47. Fica extremamente proibido o uso de e-mails que não sejam institucionais (@parauapebas.pa.gov.br) para tratar de assuntos ligados a Prefeitura de Parauapebas.

Art. 48. O uso de e-mail corporativo não garante direito sobre este, nem confere autoridade para liberar acesso a outras pessoas, pois se constitui de informações pertencentes à Prefeitura.

Art. 49. O acesso a correio eletrônico particular somente será permitido através dos navegadores de internet.

Art. 50. Os usuários são responsáveis por manter o espaço disponibilizado para o armazenamento de mensagens na sua caixa postal, evitando sua indisponibilidade. As mensagens já lidas devem ser excluídas da caixa de entrada e da lixeira.

Seção VI – Da internet

Art. 51. O setor de tecnologia poderá a qualquer tempo e sem prévio aviso suspender acesso a ferramentas de e-mail não ligadas à Prefeitura.

Art. 52. Não é permitido ao usuário utilizar-se dos serviços internos de internet do Município desvirtuando sua finalidade com o intuito de cometer fraudes.

Art. 53. Não é permitido visualizar, criar, postar, carregar ou encaminhar quaisquer arquivos ou mensagens de conteúdos abusivos, obscenos, insultuosos, sexualmente tendenciosos, pornográficos, ofensivos, difamatórios, agressivos, ameaçadores, vulgares, racistas, de apologia ao uso de drogas, de incentivos a violência ou outro material que possa violar qualquer lei aplicável.

Art. 54. Não é permitida a navegação aos sites pertencentes às categorias abaixo:

I - pornográfico e de caráter sexual;

II - compartilhamento de arquivos (ex.: peer to peer, bit torrent, emule, etc.);

III - pornografia infantil (pedofilia);

IV - apologia ao terrorismo;

V - apologia às drogas;

VI - crackers;

VII - de relacionamento;

VIII - violência e agressividade (racismo, preconceito, etc.);

IX - violação de direito autoral (pirataria, etc.);

X - áudio e vídeo, salvo com conteúdo relacionado diretamente a atividades administrativas ou profissionais;

XI - conteúdo impróprio, ofensivo, ilegal, discriminatório e similares;

XII - jogos.

Art. 55. Ficará expressamente proibido utilizar ferramentas que burlam a segurança, para usufruir serviços que não lhes são concebidos.

Art. 56. Não será permitida a manutenção não autorizada de páginas pessoais ou de serviços particulares envolvendo comercialização pela internet utilizando os recursos computacionais do Município.

Art. 57. É proibido downloads de arquivos de extensões tipo: .exe, .mp3, .wav, .bat, .com, .sys, .scr, .ppt,.mpeg, .avi, .rmvb, .dll, e de programas de entretenimento ou jogos, salvo os estritamente relacionados aos serviços inerentes à função do servidor.

Art. 58. Não é permitido o acesso a programas de TV na internet ou qualquer conteúdo sob demanda (streaming), salvo os devidamente autorizados.

Art. 59. Não será permitido o uso, para fins particulares ou de recreação, de serviços que sobrecarregam a rede computacional tais como: rádios on-line, páginas de animação, visualização de apresentações, entre outros.

Art. 60. Acessos às redes sociais só serão permitidas mediante solicitação à SEPLAN, pelo superior responsável da respectiva gerência, por meio de formulário específico disponibilizado pela mesma e com justificativa voltada ao funcionamento do trabalho a ser realizado.

Seção VII – Da assistência técnica aos recursos computacionais

Art. 61. Qualquer problema nos recursos computacionais da instituição deverá ser comunicado ao suporte técnico.

Art. 62. O servidor do suporte técnico deverá atender ao chamado de assistência técnica em até 3 (três) dias úteis da abertura do chamado.

Art. 63. O servidor do suporte técnico terá o prazo de até 5 (cinco) dias úteis, a partir do atendimento inicial, para apresentar solução ao chamado de assistência

técnica em informática, sob pena de ser considerado "concluído fora do prazo", para fins de avaliação da eficiência e eficácia do suporte.

Art. 64. A assistência técnica poderá estabelecer prioridades de atendimento sempre que necessário, de acordo com a avaliação do caso concreto.

Art. 65. Para todo atendimento de suporte técnico é necessário ter um chamado em aberto ficando proibido ao técnico o atendimento sem o mesmo.

Seção VIII – Do armazenamento de documentos e informações

Art. 66. O usuário deverá manter sigilo sobre os documentos e informações considerados estratégicos, confidenciais ou de interesse particular da Administração Pública Municipal.

Art. 67. O usuário deverá informar ao seu superior imediato quando informações ou aplicações consideradas estratégicas ou confidenciais forem encontradas sem o tratamento de segurança correto.

Art. 68. A unidade "C" não deverá ser utilizada pelo usuário para guardar documentos importantes ou confidenciais, sob o risco de perdê-los a qualquer tempo.

Art. 69. Os documentos deverão ser salvos em unidade de rede mapeadas em sua estação ou na unidade "D" de seu equipamento, quando houver.

Art. 70. Os documentos e informações geradas pelos usuários referentes às rotinas de trabalho no que diz respeito a alterações, gravações e leituras, são de inteira responsabilidade dos usuários do arquivo.

Seção IX – Das advertências e penalidades

Art. 71. Os usuários deverão estar cientes das regras e normas de uso dos recursos computacionais, evitando, desse modo, os procedimentos que prejudicam ou impedem outras pessoas de terem acesso a esses recursos ou de usá-los de acordo com o que é determinado.

Art. 72. Todo servidor que tiver conhecimento de ato ilícito praticado no uso dos recursos computacionais, assim como qualquer comportamento considerado inaceitável ou suspeito de violação dessas normas, deverá comunicar o fato imediatamente ao seu superior.

Art. 73. Sempre que julgar necessário para a preservação da integridade dos recursos computacionais e segurança da informação ou em caso de constatação e identificação de não conformidade às normas, o suporte técnico fará imediatamente o bloqueio temporário da conta de acesso e comunicará o superior imediato o teor da infração e o nome do responsável para que sejam tomadas as medidas cabíveis para a apuração dos fatos.

Art. 74. A liberação da conta de acesso somente poderá ser autorizada pelo superior imediato da pasta, por meio oficial.

Art. 75. Caso a violação de alguma norma seja passível de aplicação de penalidade, incluindo as situações consideradas graves ou reincidentes, o caso será apurado mediante a instauração de sindicância ou processo administrativo disciplinar, considerando que, sempre que tiver ciência de irregularidade no serviço público, a autoridade competente é obrigada a promover a sua apuração imediata.

Art. 76. As penalidades cabíveis ao não cumprimento das regras estabelecidas neste Decreto se aplicam a todos usuários e responsáveis técnicos, seja por omissão ou por negligência.

Seção X – Das Disposições finais

Art. 77. Todos os certificados de autenticidade, chaves de acesso, chaves seriais de softwares, mídias de instalação e demais documentos inerentes aos aspectos dos recursos de informática, devem ficar sob responsabilidade da SEPLAN, desde que previamente discutido com a equipe de tecnologia da informação.

Art. 78. O possível desconhecimento dessas normas por parte do usuário não o isenta das responsabilidades e das sanções aplicáveis nem poderá minimizar as medidas cabíveis.

Art. 79. Os casos omissos e não previstos neste Decreto deverão ser tratados junto à Secretaria Municipal de Planejamento.

Seção XI – Considerações finais

Art. 80. Os esclarecimentos adicionais a respeito deste documento poderão ser obtidos junto à SEPLAN que, por sua vez, através de procedimentos de auditoria interna, aferirá a fiel observância de seus dispositivos por parte das diversas unidades da estrutura organizacional.

Art. 81. Este Decreto entra em vigor na data de sua publicação.

Parauapebas, 24 de abril de 2018.

DARCI JOSÉ LERMEN
PREFEITO MUNICIPAL

ANEXO I

TERMO DE RESPONSABILIDADE DE UTILIZAÇÃO DE ATIVOS E RECURSOS DE INFORMÁTICA

Nome

E-mail:

Matrícula:

Eu,_____, pelo presente instrumento, na condição de servidor da Prefeitura Municipal de Parauapebas, comprometo-me a cumprir todas as orientações e determinações especificadas no Decreto Nº ___/2018 e outras editadas, em função do vínculo jurídico e funcional que tenho com o Município de Parauapebas, bem como as informações pertencentes à instituição, ou por ela custodiadas, em razão da permissão de acesso aos recursos necessários para a execução de minhas atividades profissionais, estando ciente, de acordo, aderente e responsável que devo obedecer, cumprir e respeitar as políticas, diretrizes, normas e procedimentos de segurança da informação da Prefeitura Municipal de Parauapebas, publicadas e armazenadas nos meios de comunicação internos que regem o uso dos recursos a mim disponibilizados, sejam estes digitais ou impressos, bem como o manuseio das informações a que tenho acesso, ou possa vir a ter, em decorrência da execução de minhas atividades profissionais.

Manifesto conhecimento de que descumprindo os compromissos por mim assumidos neste termo estarei sujeito às sanções aplicáveis.

Parauapebas,____ de _____de 2018.

_____

Assinatura do servidor