**DECRETO Nº 5.087, DE 27 DE NOVEMBRO DE 2018.**

*"Regulamenta o uso de recursos da Tecnologia da Informação disponibilizados pela Prefeitura Municipal da Estância Turística de Pereira Barreto, demais secretarias, repartições e autarquias".*

**JOÃO DE ALTAYR DOMINGUES,** Prefeito do Município da Estância Turística de Pereira Barreto, Estado de São Paulo, no uso de suas atribuições que lhe são conferidas por lei, e ;

**CONSIDERANDO** a necessidade de normatizar o uso apropriado dos recursos da tecnologia da informação no âmbito da Prefeitura Municipal, promovendo a proteção dos usuários, dos equipamentos, dos softwares, dos dados dos contribuintes e da própria Administração Pública;

**CONSIDERANDO** a necessidade de garantir a segurança das informações geradas, adquiridas, processadas, armazenadas e transmitidas no âmbito da Administração Municipal, de forma a atender aos princípios da confidencialidade, integridade, disponibilidade, autenticidade e legalidade;

**CONSIDERANDO** que os servidores públicos devem zelar pelas informações que lhes são confiadas no exercício de suas funções;

**D E C R E T A**

## CAPITULO I
## DAS DISPOSIÇÕES PRELIMINARES

**Art. 1º** Fica instituída a Política de Segurança da Informação no âmbito da Prefeitura Municipal da Estancia Turística de Pereira Barreto bem como as demais secretarias, repartições e autarquias.

**§ 1º** A política de Segurança da Informação define as práticas a serem seguidas na Prefeitura Municipal da Estância Turística de Pereira Barreto, demais secretarias, repartições e autarquias, de forma a minimizar os riscos à segurança das informações, bem como para assegurar os altos padrões de qualidade na prestação dos serviços da instituição.

**§ 2º** Compete à Secretaria de Administração a coordenação das políticas de gestão da segurança da informação no Município.

**Art. 2º** Para efeito deste Decreto ficam estabelecidos os seguintes conceitos:

**I - Agente Público** - Servidores, estagiários e prestadores de serviços que estejam exercendo atividades públicas municipais.

**II - Recursos de TI** - Quaisquer equipamentos ou dispositivos que utilizem tecnologia da informação, bem como quaisquer recursos ou informações que sejam acessíveis através desses equipamentos ou dispositivos tecnológicos, tais como impressoras, sistemas, programas, acessos à rede local, internet, VPN, pendrive, smartcard, tokens, smartphones, roteadores, desktops e pastas compartilhadas.

**III - Sistema de Informação** - Aplicação da tecnologia da informação que dá apoio às atividades de determinada área de conhecimento, com o fim de otimizar as operações, o gerenciamento e a decisão, trabalhando os dados e transformando em informação.

**IV - Credenciais de Acesso** - Conjunto composto pelo nome de conta e respectiva senha utilizado para ingresso ou acesso (login) em equipamentos, rede ou sistema.

**V - Log**: registro de atividades gerado por programa de computador que possibilita a reconstrução, revisão e análise das operações, procedimento ou evento em sistemas de informação;

**Art. 3º** Compete ao Setor de Tecnologia da Informação:

**I –** Elaborar e revisar continuamente os procedimentos e a normatização relacionada ao processo de gestão da segurança da informação;

**II –** Avaliar propostas de modificação da Política de Segurança da Informação encaminhadas pelos demais órgãos administrativos da Administração Municipal;

**III** – Planejar, elaborar e propor estratégias e ações para institucionalização da política, normas e procedimentos relativos à segurança da informação;

**IV -** Avaliar a eficácia dos procedimentos relacionados à segurança da informação, propondo e implementando medidas que visem a melhoria do processo de gestão da segurança da informação;

**V -** Apurar os incidentes de segurança críticos e dar o encaminhamento adequado;

**VI -** Avaliar, indicar, propor e fiscalizar as compras dos recursos de TI;

**Art. 4º** Compete ao Chefe da Tecnologia da Informação complementarmente às demais diretrizes estabelecidas neste Decreto:

**I** – Subsidiar o processo de classificação da informação, de forma a viabilizar a correta definição a ela relacionada;

**II** – Responsabilizar-se pela exatidão, integridade e atualização da informação sob sua custódia;

**III** – Subsidiar o Setor de Tecnologia da Informação na compatibilização de estratégias, planos e ações desenvolvidos no âmbito da Administração Municipal relativos a segurança da informação;

**IV –** Realizar análise de riscos em processos, em consonância com os objetivos e ações estratégicas estabelecidas pelo Poder Executivo, e atualizá-la periodicamente;

**V –** Relatar os incidentes de segurança da informação para que sejam tomadas as devidas providências em conjunto com as áreas diretamente envolvidas;

**Art. 5º** O cadastro de usuário para acesso aos recursos da Tecnologia da Informação, deverá ser solicitado pela chefia imediata ao Setor de Tecnologia da Informação para providências quanto ao cadastramento.

## CAPITULO II
## DO AGENTE PÚBLICO

**Art. 6º** As credenciais de acesso a rede e demais recursos da tecnologia da informação, são de uso pessoal e intransferível, sendo que toda a e qualquer ação executada por meio de um determinado usuário, será de responsabilidade daquele a quem o login foi atribuído, cabendo-lhe, portanto, zelar pela confidencialidade de sua senha.

**Art. 7º** Ao perder o vínculo com a Prefeitura todos os acessos do usuário aos recursos da tecnologia da informação serão excluídos, suas contas de e-mails canceladas e seu conteúdo apagado.

**Parágrafo único**. Fica a Secretaria de Administração, através da Diretoria de Recursos Humanos, responsável por repassar à Setor de Tecnologia da Informação, a qualquer tempo, as demissões/exonerações, do quadro de funcionários, para que as providências acima sejam tomadas.

**Art. 8º** É dever do agente público, em consonância com a Política de Segurança da Informação estabelecida neste Decreto:

**I –** Zelar pelo sigilo da sua senha;

**II** – Zelar pela segurança das informações, fechando ou bloqueando o acesso aos equipamentos de informática ou softwares quando estiver utilizando;

**III** – Comunicar imediatamente ao seu superior hierárquico qualquer suspeita de que estejam sendo executados atos em seu nome por meio dos recursos da tecnologia da informação;

**IV** – Zelar pela integridade física dos equipamentos de informática utilizados, evitando submetê-los a condições de riscos, mantendo os afastados de líquidos e alimentos, não danificando as placas de patrimônio, não colando qualquer tipo de adesivo nos equipamentos ou qualquer material e/ ou utensílio que possa danificá-los, e comunicando ao órgão competente qualquer anormalidade ou defeito;

**V** – Zelar pela segurança da informação que esteja sob sua custódia em razão de seu exercício funcional.

**Art. 9º** É proibido aos usuários:

**I** – Fornecer por qualquer motivo, suas credenciais para acesso a outrem;

**II** – Fazer uso das credenciais de terceiro;

**III** – Utilizar os recursos da tecnologia da informação em desacordo com os princípios éticos da Administração Pública;

**IV** – Visualizar, acessar, expor, armazenar, distribuir, editar ou gravar material de natureza pornográfica, racista, jogos, música, filmes e outros relacionados, por meio de uso de recursos de computadores da Prefeitura;

**V –** Fazer cópias não autorizadas dos softwares desenvolvidos ou adquiridos pela Prefeitura.

## CAPITULO III
## DA UTILIZAÇÃO DA REDE

**Art. 10** Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta, incluindo acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes

**Art. 11** Não são permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques do tipo "negativos de acesso", provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "quebrar" (invadir) um servidor.

**Art. 12** Não é permitido o uso de qualquer tipo de programa ou comando designado a interferir com sessão de usuário.

**Art. 13** Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas acessados, evitando, desta maneira, o acesso por pessoas não autorizadas e efetuar o logout/logoff da rede ou bloqueio do desktop através de senha.

**Art. 14** Não é permitido criar e/ou remover arquivo fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas;

**Art. 15** A pasta Temporária, não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível;

**Parágrafo único.** Haverá limpeza semanal dos arquivos armazenados na pasta Temporária, para que não haja acúmulo desnecessário de arquivos.

**Art. 16** É obrigatório armazenar os arquivos inerentes à prefeitura no servidor de arquivos para garantir o backup dos mesmos.

## CAPITULO III
## DA UTILIZAÇÃO DO E-MAIL

**Art. 17** O usuário, a critério de seu chefe imediato e de acordo com as necessidades de serviço, poderá ter acesso a uma conta de correio eletrônico associada ao respectivo login.

**§ 1°** As contas oficiais de e-mail da Prefeitura (@pereirabarreto.sp.gov.br), devem ser utilizadas, exclusivamente, para transmitir e receber informações relacionadas às atividades administrativas.

**§ 2°** As contas de e-mail particulares não terão suporte da Setor de Tecnologia da Informação, podendo ser bloqueado o acesso sem prévio aviso.

**Art. 18** É considerado uso inadequado ao serviço de e-mail:

**I -** Acessar contas de e-mail de outros usuários;

**II -** Enviar material ilegal ou não ético, comercial com mensagens do tipo corrente, spam, entretenimento e outros que não sejam de interesse da Prefeitura, bem como campanhas político-partidárias e que tenham finalidade eleitoreira;

**III-** Enviar e-mail a qualquer pessoa que não o deseje receber. Se o destinatário solicitar a interrupção de envio e-mails, o usuário deve acatar tal solicitação e não lhe enviar qualquer e-mail;

**IV -** Enviar de e-mail mal-intencionado, tais como "mail-bombing" ou sobrecarregar um usuário, site ou servidor com e-mail muito extenso ou numerosas partes de e-mail;

**V -** Forjar qualquer das informações do cabeçalho do remetente;

**VI -** Enviar mensagens que possam afetar de forma negativa a Prefeitura e seus servidores públicos.

**Art. 19** É proibido o envio de grande quantidade de mensagens de e-mail ("junk mail" ou "spam") que, de acordo com a capacidade técnica da Rede, seja prejudicial ou gere reclamações de outros usuários. Isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política;

**Parágrafo único.** O setor de imprensa, a Assessoria de Comunicação e o Setor de Tecnologia da Informação, são os únicos e exclusivos setores que poderão fazer o envio de mala direta.

**Art. 20** As contas de e-mail terão limitado de espaço para armazenamento de mensagens, devendo o usuário efetuar a exclusão das mensagens inutilizadas, sob pena de ficar impedido automaticamente de enviar e receber novas mensagens, devendo casos excepcionais serem encaminhados à Diretoria de Tecnologia da Informação para análise e deliberação.

**§ 1°** As mensagens enviadas ou recebidas, incluindo seus anexos, tem limitação de tamanho, sendo automaticamente bloqueadas quando ultrapassarem esse limite.

**§ 2°** Os anexos às mensagens enviadas e recebidas não devem conter arquivos que não estejam relacionados às atividades administrativas ou que ponham em risco a segurança do ambiente da rede local.

**Art. 21** É obrigatória a manutenção da caixa de e-mail, enviando acúmulo de e-mails e arquivos inúteis.

## CAPITULO III
## DA UTILIZAÇÃO DE ACESSO A INTERNET

**Art. 22** É considerado uso inadequado da internet:

**I -** Acessar informações consideradas inadequadas ou não relacionadas às atividades administrativas, especialmente sites de conteúdo agressivo (racismo, pedofilia, nazismo, etc.), de drogas, pornografia e outros relacionados;

**II** – Realizar download de arquivos e outros que possam tornar a rede local vulnerável a invasões externas e ataques a programas de código malicioso em suas diferentes formas;

**III** – Tentar ou efetivamente burlar as regras definidas de acesso à internet;

**IV** - Utilizar acesso à internet provido pela Prefeitura para transferência de arquivos que não estejam relacionados às suas atividades;

**V** – Divulgar informações confidenciais da Prefeitura em grupos de discussão, listas ou bate-papos, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas na forma da lei.

**VI** - Utilizar softwares de peer-to-peer (P2P), tais como Kazaa, Morpheus, Emule, Torrents e afins

**Art. 23** É proibido a divulgação de informações confidenciais da prefeitura em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou forma da lei.

**Art. 24** Os Funcionários com acesso à Internet não podem efetuar uploads de qualquer software licenciado à prefeitura ou de dados de propriedade da prefeitura ou de seus clientes, sem expressa autorização do gerente responsável pelo software ou pelos dados

**Art. 25** Caso o Setor de Tecnologia da Informação julgue necessário, haverá bloqueios de acesso à:

**I -** Arquivos que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;

**II -** Domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;

**Art. 26** Haverá geração de LOG dos sites acessados por usuário e se necessário a publicação desse relatório.

**Art. 27** É Proibido o uso de rede sociais durante o expediente. Usuários que tenham esse acesso liberado, desde já, fiquem cientes que o acesso será monitorado para que não haja futuros transtornos.

## CAPITULO IV
## CONSIDERAÇÕES FINAIS

**Art. 28** É vedado o uso de equipamentos de informática particulares conectados à rede de informática da Prefeitura, sem a prévia autorização da Diretoria de Tecnologia da Informação.

**Parágrafo único**. Em todos os equipamentos utilizados na rede da Prefeitura, será instalado software de acesso remoto, sendo que a desinstalação do mesmo pelo usuário acarretará na retirada do equipamento da rede e envio de notificação ao superior hierárquico do usuário.

**Art. 29** O Setor de Tecnologia da Informação é a único detentor e responsável pela senha de administrador dos equipamentos.

**Art. 30** São considerados usos inadequados dos equipamentos de informática:

**I** – Instalar hardware em computador da Prefeitura;

**II** – Instalar softwares de qualquer espécie em computador da Prefeitura, secretaria e/ou departamentos

**III –** Reconfigurar a rede corporativa ou inicializa-la sem prévia autorização expressa;

**IV** – Efetuar montagem, alteração, conserto ou manutenção em equipamentos da Prefeitura sem o conhecimento do Setor de Tecnologia da Informação;

**V** – Alterar o local de instalação dos equipamentos/ hardwares de informática, sem prévia autorização;

**VI** – Instalar dispositivo ou utilizar internet móvel, sem prévia autorização expressa;

**VII** – Conectar equipamento particular na rede de computadores da Prefeitura, sem prévia autorização expressa;

**VIII** – Utilizar mecanismos para burlar o usuário/ administrador, concedendo privilégios aos demais usuários;

**IX** – Utilizar dispositivos de armazenamento externos tais como pen drive, HD externo, sem prévia autorização,

**Art. 31** Todo o chamado de suporte deverá ser feito pelo sistema de chamados que se encontra no sitio eletrônico https://suporte.pereirabarreto.sp.gov.br.

**§ 1°** Os chamados serão atendidos conforme ordem de abertura e prioridade, definidos pelo setor de Tecnologia de Informação;

**§ 2°.** Os chamados serão resolvidos remotamente e só após esgotadas as tentativas ou quando necessário, de forma presencialmente;

**§ 3° -** Na dificuldade do setor de Informática de se deslocar até o local, fica responsável cada secretaria, diretoria ou setor, de trazer o equipamento para o reparo até o Setor de Tecnologia da Informação

**Art. 32** Todo caso de exceção às determinações da Política de Segurança da Informação deve ser analisado de forma individual, aplicável apenas ao seu solicitante, dentro dos limites e motivos que o fundamentaram.

**Art. 33** A não observância da Política de Segurança da Informação pelos usuários configura descumprimento de dever funcional, indisciplina ou insubordinação, conforme o caso, sujeitando o infrator à incidência das sanções cabíveis, nos termos da legislação vigente.

**Art. 34** Este Decreto entra em vigor na data de sua publicação, revogadas as disposições em contrário.

Paço Municipal "Francisco Vidal Martins", 27 de novembro de 2018.

**JOÃO DE ALTAYR DOMINGUES**
**Prefeito Municipal**

Registrado e publicado nesta
Secretaria na data supra