**DECRETO Nº 3930, DE 04 DE OUTUBRO DE 2022.**

Regulamenta o uso de recursos da Tecnologia da Informação disponibilizados pela Prefeitura da Estância Turística de Paraibuna, e dá outras providências.

**VICTOR DE CASSIO MIRANDA**, Prefeito da Estância Turística de Paraibuna, Estado de São Paulo, usando das atribuições que lhe são conferidas por Lei,

**CONSIDERANDO** a necessidade de normatizar o uso apropriado dos recursos da tecnologia da informação no âmbito da Prefeitura da Estância Turística de Paraibuna, 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;

**CONSIDERANDO** que as ações de segurança da informação reduzem custos e riscos e aumentam os benefícios prestados aos cidadãos, ao permitir a oferta de processos, produtos e serviços suportados por sistemas de informações mais seguros;

**DECRETA:**

**Art. 1° -** Fica instituída a Política de Segurança da Informação no âmbito da Prefeitura da Estância Turística de Paraibuna.

**§ 1° -** A Política de Segurança da Informação constitui um conjunto de diretrizes e normas que estabelecem o princípio de proteção, controle e monitoramento das informações processadas, armazenadas e custodiadas pela Administração Municipal, aplicando-se a todos os órgãos do Poder Executivo Municipal.

**§ 2° -** Compete ao Departamento Municipal de Administração e Finanças a coordenação das políticas de gestão da segurança da informação no Município.

Art. 2°- Para efeitos deste Decreto ficam estabelecidos os seguintes conceitos:

**I -** Autenticidade: garantia que a informação é procedente e fidedigna, capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu;

**II -** Confidencialidade: garantia de que as informações sejam acessadas e reveladas somente a indivíduos, órgãos, entidades e processos devidamente autorizados;

**III -** Dado: parte elementar da estrutura do conhecimento, computável, mas incapaz de, por si só, gerar conclusões inteligíveis ao destinatário;

**DECRETO Nº 3930, DE 04 DE OUTUBRO DE 2022.**

**IV -** Disponibilidade: garantia de que as informações e os recursos de tecnologia da informação estejam disponíveis sempre que necessário mediante a devida autorização para seu acesso ou uso;

**V -** Gestor da informação: pessoa detentora de competência institucional; para autorizar ou negar acesso à determinada informação ao usuário;

**VI -** Incidente de segurança da informação: um evento ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

**VII -** Informação: conjunto de dados que, processados ou não, podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

**VIII -** Integridade: garantia de que as informações estejam protegidas contra manipulações e alterações indevidas;

**IX -** Legalidade: garantia de que todas as informações sejam criadas e gerenciadas de acordo com a legislação em vigor;

**X -** Login ou ID de usuário: identificação única do usuário, permitindo o seu acesso e controle na utilização dos recursos da tecnologia da informação;

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

**XII -** Não repúdio: garantia de que um usuário não consiga negar uma operação ou serviço que modificou ou criou uma informação;

**XIII -** Recursos da tecnologia da informação: recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar a informação, dentre estes podemos destacar os computadores, notebooks, tablets, pendrives, mídias, impressoras, scanners, softwares etc.

**XIV -** Risco: combinação de probabilidades da concretização de uma ameaça e seus potenciais impactos;

**XV -** Segurança da informação: preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas;

**XVI -** Senha: conjunto alfanumérico de caracteres destinado a assegurar a identidade do usuário e permitir seu nível de acesso aos recursos da tecnologia da informação não disponíveis ao público, de uso pessoal e intransferível;

**XVII -** Tecnologia da informação e comunicação: solução ou conjunto de soluções sistematizadas baseadas no uso de recursos tecnológicos que visam resolver problemas relativos à geração, tratamento, processamento, armazenamento, veiculação e reprodução de dados, bem como subsidiar processos que convertem dados em informação;

**XVIII -** Usuário: funcionário, servidor, comissionado, estagiário, prestador de serviço, terceirizado, conveniado, credenciado, fornecedor ou qualquer outro indivíduo ou organização que venham a ter relacionamento, direta ou indireta, com os órgãos e entidades da Administração Municipal;

**DECRETO Nº 3930, DE 04 DE OUTUBRO DE 2022.**

**XIX -** Violação: qualquer atividade que desrespeite as diretrizes estabelecidas nesta política ou em quaisquer das demais normas que a complemente.

**Art. 3º -** Constituem objetivos da Política de Segurança da Informação:

**I -** Dotar a Prefeitura da Estância Turística de Paraibuna de instrumento jurídico, normativo e institucional que a capacite de forma técnica e administrativa, com o objetivo de assegurar a confidencialidade, a integridade, a autenticidade, o não repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sigilosas da Administração Municipal;

**II -** Estabelecer e controlar os níveis de acesso de fornecedores externos aos sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;

**III -** Assegurar a interoperabilidade entre os sistemas de segurança da informação;

**IV -** Incorporação da cultura da segurança da informação, por todos os usuários, como um elemento essencial em seus hábitos e atitudes dentro e fora da organização.

**Art. 4º -** A Política de Segurança da Informação instituída neste Decreto reger-se-á pelos seguintes princípios:

**I -** Tratamento da informação como patrimônio, tendo em vista que a divulgação das informações estratégicas de qualquer natureza pertencente à Administração deve ser protegida de forma adequada, com vistas a evitar alterações, acessos ou destruição indevidos;

**II -** Classificação da informação, garantindo-lhe o adequado nível de proteção, considerando:

**a)** a avaliação da necessidade do tipo de acesso pelo usuário, adotando-se como parâmetro o grau de confidencialidade da informação;

**b)** a definição de confidencialidade da informação em consonância com as atividades desempenhadas pelo usuário, com vistas a garantir a adequada autorização de acesso pelo gestor da informação, que deverá conter os limites de acesso, tais como leitura, atualização, criação e remoção, entre outros.

**III -** Controle de acesso às informações, tendo como orientação a classificação definida no inciso II deste artigo, respeitando a legislação vigente e considerando, ainda, que:

**a)** o acesso e o uso de qualquer informação, pelo usuário, devem ser restringidos ao necessário para o desempenho de suas atividades;

**b)** no caso de acesso a sistemas informatizados, deverão ser utilizados sistemas e tecnologias autorizadas pela Administração, por meio de usuário e senha, ambos pessoais e intransferíveis.

**IV -** Continuidade do uso da informação, sendo necessária, para o funcionamento dos sistemas, pelo menos uma cópia de segurança atualizada e guardada em local remoto, com nível de proteção equivalente ao nível de proteção da informação original, observada as seguintes regras:

**a)** para a definição das cópias de segurança devem ser considerados os aspectos legais, históricos, de auditoria e de recuperação de ambiente;

**DECRETO Nº 3930, DE 04 DE OUTUBRO DE 2022.**

**b)** os recursos tecnológicos, de infraestrutura e os ambientes físicos utilizados para suportar os sistemas de informação devem ter controle de acesso físico, condições ambientais adequadas e ser protegidos contra situações de indisponibilidade causadas por desastres ou contingências;

**c)** definição do nível de disponibilidade para cada serviço prestado pelos sistemas de informação, nas situações mencionadas na alínea "b" deste inciso.

**V -** Educação em segurança da informação, devendo ser observado pelo usuário a correta utilização das informações e dos recursos computacionais disponibilizados.

**Art. 5°** - As medidas a serem adotadas para fins de proteção da informação deverão considerar:

**I -** Os níveis adequados de integridade, confidencialidade e disponibilidade da informação;

**II -** A compatibilidade entre a medida de proteção e o valor do ativo protegido;

**III -** O alinhamento com as diretrizes da Administração Municipal;

**IV -** As melhores práticas para a gestão da segurança da informação;

**V -** Os aspectos comportamentais e tecnológicos apropriados.

**Art. 6°** - Compete a Divisão de Gestão Administrativa 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 -** Garantir que os registros de auditoria de eventos de segurança da informação sejam produzidos e mantidos em conformidade com as normas vigentes;

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

**V -** Avaliar a eficácia dos procedimentos relacionados à segurança de informação, propondo e implementando medidas que visem a melhoria do processo de gestão da segurança da informação no âmbito da Administração Municipal;

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

**VII -** Promover a conscientização, o treinamento e a educação em segurança da informação.

**Art. 7°** - Compete ao gestor 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;

**DECRETO Nº 3930, DE 04 DE OUTUBRO DE 2022.**

**III -** Subsidiar a Divisão de Gestão Administrativa na compatibilização de estratégias, planos e ações desenvolvidos no âmbito da Administração Municipal relativos à 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. 8º -** O cadastro de usuário para acesso aos recursos da tecnologia da informação depende de prévia autorização da chefia imediata encaminhado à Divisão de Gestão Administrativa para providências quanto ao cadastramento.

**§ 1º -** Ao usuário será fornecido o "login ou ID do usuário", sobre o que deverá tomar ciência e, assim, assinar o termo de responsabilidade de acesso aos recursos da tecnologia da informação.

**§ 2º -** Após o cadastro, o usuário deverá registrar uma senha, de uso pessoal e intransferível, que deverá ser alterada periodicamente, a qual permitirá seu login na rede de computadores da Prefeitura da Estância Turística de Paraibuna e o acesso aos recursos da tecnologia da informação.

**§ 3º -** Qualquer mudança de lotação dos usuários deverá ser comunicada imediatamente pelo Departamento de origem, através da chefia imediata, à Divisão de Gestão Administrativa para que sejam realizados os ajustes necessários ao cadastro.

**§ 4º -** Qualquer mudança que venha a ocorrer no perfil do usuário, seja de alteração do perfil de acesso, ampliação ou exclusão de permissões deve ser comunicada pela chefia imediata.

**Art. 9º -** O login na rede e os 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. 10 -** Ao perder o vínculo com a Prefeitura da Estância Turística de Paraibuna, 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 -** Ficam os Departamento Municipais responsáveis por repassar à Divisão de Gestão Administrativa, a qualquer tempo, as demissões/exonerações, do quadro de servidores, para que as providências acima sejam tomadas.

**Art. 11 -** É dever do usuário, 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 não 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;

**DECRETO Nº 3930, DE 04 DE OUTUBRO DE 2022.**

**IV -** Zelar pela integridade física dos equipamentos de informática utilizados, evitando submetê-los a condições de riscos, mantendo 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. 12 -** É proibido aos usuários:

**I -** Fornecer por qualquer motivo, seu login e senha para acesso a outrem;

**II -** Fazer uso do login e da senha 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 da Estância Turística de Paraibuna;

**V -** Acessar sites ou serviços que representem risco aos dados ou à estrutura de redes da Prefeitura da Estância Turística de Paraibuna

**VI -** Fazer cópias não autorizadas dos softwares desenvolvidos ou adquiridos pela Prefeitura da Estância Turística de Paraibuna;

**VII -** Fazer cópias reprográficas de documentos particulares utilizando os equipamentos da Prefeitura da Estância Turística de Paraibuna.

**Art. 13 -** É vedado o uso de equipamentos de informática particulares conectados à rede de informática da Prefeitura da Estância Turística de Paraibuna, sem a prévia autorização da Divisão de Gestão Administrativa.

**Art. 14 -** A Divisão de Gestão Administrativa é a única detentora responsável pela senha de administrador dos equipamentos.

**Parágrafo único -** As solicitações para compartilhamento da senha de administrador dos equipamentos deverão ser encaminhadas com a devida justificativa para que seja avaliada esta necessidade em conjunto com órgão solicitante.

**Art. 15 -** São considerados usos inadequados dos equipamentos de informática:

**I -** Instalar hardware em computador da Prefeitura da Estância Turística de Paraibuna;

**II -** Instalar softwares de qualquer espécie em computador da Prefeitura da Estância Turística de Paraibuna;

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

**IV -** Efetuar montagem, alteração, conserto ou manutenção em equipamento da Estância Turística de Paraibuna sem o conhecimento da Divisão de Gestão Administrativa

**DECRETO Nº 3930, DE 04 DE OUTUBRO DE 2022.**

**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 da Estância Turística de Paraibuna, sem prévia autorização expressa;

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

**IX -** Utilizar equipamento de impressora da Prefeitura da Estância Turística de Paraibuna para a impressão de documento não oficial ou não relacionado a processo de interesse da Administração.

**Art. 16 -** Compete exclusivamente a Divisão de Gestão Administrativa realizar backup diário dos dados armazenados nos servidores internos da Prefeitura.

**§ 1º -** Não compete a Divisão de Gestão Administrativa fazer backup diário ou periódico de informações armazenadas localmente nos computadores da Prefeitura da Estância Turística de Paraibuna.

**§ 2º -** A Divisão de Gestão Administrativa deverá orientar os usuários quanto as melhores práticas para realização de backups para aplicativos instalados em computadores locais e quanto a importância de salvar os arquivos mais importantes na rede da Prefeitura da Estância Turística de Paraibuna.

**Art. 17 -** A Prefeitura Municipal da Estância Turística de Paraibuna adotará política interna de inspeção e restrição de acesso à internet, com a identificação do usuário por meio de sistema automatizado.

**Art. 18 -** 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 -** Fazer download de arquivos e outros que possam tornar a rede local vulnerável a invasões externas e ataques a programas de código maliciosos em suas diferentes formas;

**III -** Violar os sistemas de segurança da Prefeitura da Estância Turística de Paraibuna;

**IV -** Tentar ou efetivamente burlaras regras definidas de acesso à internet;

**V -** Alterar os registros de acesso à internet;

**VI -** Realizar ataque ou invadir computadores da Prefeitura da Estância Turística de Paraibuna;

**VII -** Utilizar acesso à Internet provido pela Prefeitura da Estância Turística de Paraibuna para transferência de arquivos que não estejam relacionados as suas atividades;

**VIII -** Divulgar informações confidenciais da Prefeitura da Estância Turística de Paraibuna em grupos de discussão, listas ou bate-papos, não importando se a divulgação foi deliberada ou inadvertida, sob pena de sofrer os sansões previstas na forma da lei.

**DECRETO Nº 3930, DE 04 DE OUTUBRO DE 2022.**

**Art. 19 -** O chefe imediato do usuário deverá comunicar quaisquer ações que comprometam a segurança, a integridade, o desempenho e a descaracterização de equipamentos e redes da Prefeitura da Estância Turística de Paraibuna.

**Art. 20 -** 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 da Estância Turística de Paraibuna deverão ser utilizadas, exclusivamente, para transmitir e receber informações relacionadas às atividades administrativas.

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

**Art. 21 -** As contas de e-mail terão limitação 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 Divisão de Gestão Administrativa para análise e deliberação.

**§ 1° -** As mensagens enviadas ou recebidas, incluindo seus anexos, terão 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. 22 -** É considerado uso inadequado do 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 mensagens que possam afetar de forma negativa a Prefeitura da Estância Turística de Paraibuna, seus servidores públicos ou agentes públicos.

**Art. 23 -** Os usos de softwares de compartilhamento de arquivos e de troca de mensagens serão tratados em Decreto específico.

**Art. 24 -** 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. 25 -** Os equipamentos de impressão da Prefeitura da Estância Turística de Paraibuna devem ser utilizados, exclusivamente, para a impressão de documentos oficiais ou relacionados à Administração.

**Parágrafo único -** Os equipamentos serão conectados à rede e serão utilizados mediante inserção da senha do usuário cadastrado.

**DECRETO Nº 3930, DE 04 DE OUTUBRO DE 2022.**

**Art. 26 -** A não observância da Política de Segurança da Informação pelos usuários configura descumprimento de dever funcional, com enquadramento no art. 181, incisos III e VIII, e art. 182, inciso XV, ambos da Lei Complementar nº 75, de 31 de julho de 2018, sem prejuízo de outros, sujeitando o infrator à incidência das sanções cabíveis, nos termos da legislação vigente.

**Art. 27 -** O Comitê Gestor de Segurança da Informação - CGSI será designado por Portaria do Chefe do Poder Executivo, composto por 15 (quinze membros, sendo 02 (dois) representantes, 01 (um) titular e 01 (um) suplente de cada departamento da Prefeitura Municipal, nos seguintes termos:

**I -** Presidente;

**II -** Departamento Municipal de Administração e Finanças;

**a -** Titular

**b-** Suplente

**III -** Departamento Municipal de Educação;

**a -** Titular

**b-** Suplente

**IV -** Departamento Municipal de Assistência Social;

**a -** Titular

**b -** Suplente

**V -** Departamento Municipal de Serviços Municipais;

**a -** Titular

**b -** Suplente

**VI -** Departamento Municipal de Planejamento, Gestão e Turismo;

**a -** Titular

**b -** Suplente

**VII -** Departamento Municipal de Agricultura, Abastecimento e Meio Ambiente.

**a -** Titular

**b -** Suplente

**VIII -** Departamento Municipal de Saúde.

**a -** Titular

**b -** Suplente

**Art. 28 -** Este Decreto entra em vigor na data de sua publicação, revogadas as disposições em contrário.

Paraibuna, 04 de outubro de 2022.

**VICTOR DE CASSIO MIRANDA**
Prefeito Municipal

Registrado e publicado na Secretaria da Prefeitura Municipal, na data supra.
Dair Aparecida Santos Araújo
Assessora da Secretaria de Gabinete