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;