DECRETO Nº. 4.706, DE 10 DE MAIO DE 2022.

CRIA, NO ÂMBITO DA PREFEITURA MUNICIPAL DE ITAGUAÍ, A POLÍTICA DE SEGURANÇA DA INFORMAÇÃOE PRIVACIDADE, E DÁ OUTRAS PROVIDÊNCIAS.

O PREFEITO DO MUNICÍPIO DE ITAGUAÍ-RJ, no uso de suas atribuições legais, de acordo com os arts. 99, VII, e 123, I, *i*, ambos da Lei Orgânica do Município de Itaguaí,

DECRETA:

Art. 1º. Fica criada, no âmbito da Prefeitura Municipal de Itaguaí, a Política de Segurança da Informação e Privacidade,nos termos do Anexo.

Art. 2º. Este Decreto entra em vigor na data de sua publicação, revogando qualquer disposição em contrário.

Registre-se, publique-se e cumpra-se.

(a) RUBEM VIEIRA DE SOUZA
Prefeito Municipal

Prefeitura Municipal de Itaguaí

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Versão.1.0.

Sumário

OBJETIVO

O objetivo desta Política de Segurança da Informação e Privacidade é estabelecer diretrizes que permitam aos colaboradores da Prefeitura Municipal de Itaguaí seguirem padrões de comportamento relacionados à segurança da informação e privacidade de dados, adequados ao desempenho das atividades da administração, em consonância com as normas ABNT NBR ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação e ISO/IEC 27701 – Sistema de Gestão da Privacidade da Informação, a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/ 2018, o Decreto Federal nº 10.222/2020, que aprova a Estratégia Nacional de Segurança Cibernética e o Marco Civil da Internet, Lei nº 12.965/2014, preservando as informações no tocante a:

- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que os dados não estarão disponíveis e nem serão divulgados a indivíduos, entidades ou processos sem autorização.

As informações de propriedade da Prefeitura Municipal de Itaguaí, ou sob a sua guarda, constituem-se patrimônio local, sendo essenciais ao desempenho das atividades de sua competência e tomada de decisões estratégicas.

Dessa forma, busca-se desenvolver um comportamento ético e profissional, para que todos possam utilizar, da melhor forma, as ferramentas de TI e as informações por elas geradas, seja em meio físico ou digital, ao mesmo tempo, busca-se reduzir ameaças através da adoção de medidas preventivas para evitar possíveis incidentes que tragam prejuízos à instituição.

1) CONCEITOS E DEFINIÇÕES

Para os fins dessa Política, considera-se:

- **Acesso Não Autorizado** – Acesso indevido ou não previsto, obtido por quaisquer meios, procedimentos e a qualquer título, à revelia da política ou do controle de acesso vigentes, ou ainda decorrente de falhas ou imperfeições nos mecanismos de controle de acesso.
- **Acesso Lógico** – acesso a redes de computadores, sistemas e estações de trabalho por meio de autenticação;
- **Acesso Remoto** – ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário;
- **Ameaça** – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
- **Análise/avaliação de riscos** – processo completo de análise e avaliação de riscos;
- **Ativo** – qualquer bem, tangível ou intangível, que tenha valor para a organização;
- **Ativo de Tecnologia da Informação (TI)** – são os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles tem acesso;
- **Auditoria** – verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;
- **Autenticação** – é o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira;
- **Autenticidade** – propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
- **Banco de Dados (ou Base de Dados)** – é um sistema de armazenamento de dados, ou seja, um conjunto de registros com o objetivo de organizar e guardar as informações;

- **Bloqueio de acesso** – processo que tem por finalidade suspender temporariamente o acesso;
- **Classificação da informação** – atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;
- **Colaborador** – servidores, funcionários, empregados, contratados por tempo determinado, estagiários e prestadores de serviços que exercem atividades no âmbito da Prefeitura Municipal de Itaguaí;
- **Confidencialidade** – propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizada/credenciada;
- **Contingência** – descrição de medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à instituição;
- **Controle de Acesso** – conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
- **Cópia de Segurança (Backup)** – Gravação de dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade;
- **Credenciais ou contas de acesso** – permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e lógica como identificação de usuário e senha;
- **Criptografia** – é o Mecanismo de proteção da informação mediante sua transformação em um texto cifrado (criptografado), de maneira que somente os possuidores da chave de decifragem podem reverter a cifragem para tornar o texto inteligível novamente;
- **Dado** – representação de uma informação, instrução, ou conceito, de modo que possa ser armazenado e processado por um computador;

- **Disponibilidade** – propriedade que busca garantir que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
- **Download** – (baixar) copiar arquivos de um servidor (site) na internet para um computador;
- **Gestão de Continuidade de Negócios** – processo de gestão global que identifica potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizando, poderiam causar, e fornecendo e mantendo um nível aceitável de serviço em face de rupturas e desafios à operação normal do dia a dia;
- **Gestão de Risco** – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;
- **Gestão de Segurança da Informação e Privacidade** – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;
- **Hardware** – é a parte física do computador, conjunto de componentes eletrônicos, circuitos integrados e periféricos, como a máquina em si, placas, impressora, teclado e outros;
- **Incidente de Segurança** – é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
- **Informação** – dados, processados ou não, que podem ser utilizados para a produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- **Informação sigilosa** – informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da

sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

- **Integridade** – propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- **Internet** – rede mundial de computadores;
- **Intranet** – rede de computadores privada que faz uso dos mesmos protocolos da Internet. Pode ser entendida como rede interna de alguma instituição em que geralmente o acesso ao seu conteúdo é restrito;
- **Log** – é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais;
- **Logon** – procedimento de identificação e autenticação do usuário nos recursos de tecnologia da Informação. É pessoal e intransferível;
- **Norma** – documento interno que regulamenta formal e administrativamente, de maneira geral ou específica, aspectos ou diretrizes expressas na PSIP, no todo ou em parte da instituição. As normas mapeiam a PSIP na organização técnico- administrativa da instituição, estabelecendo regras para a sua implementação;
- **Peer-to-peer (P2P)** – (Ponto a ponto) permite conectar o computador de um usuário a outro, para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, entre outros;
- **Perfil de acesso** – conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;
- **Política de Segurança da Informação e Privacidade (PSIP)** – documento aprovado pela autoridade responsável pelo órgão, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e privacidade na instituição;

- **Protocolo** – convenção ou padrão que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais. Método padrão que permite a comunicação entre processos, conjunto de regras e procedimentos para emitir e receber dados numa rede;
- **Recursos Computacionais** – recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;
- **Rede Corporativa** – conjunto de todas as redes locais sob a gestão da instituição;
- **Responsabilidade** – obrigações e deveres decorrentes da legislação vigente, ofício, cargo, função ou por força de contrato, na proteção dos ativos de informação de qualquer natureza;
- **Senha ou Credencial de Acesso** – credencial que concede, de maneira prevista, o direito de acesso, físico ou lógico, a determinado ativo de informação de qualquer natureza, ou local que o abrigue. Uma senha ou credencial fraca é toda aquela que não obedece aos critérios e requisitos mínimos de qualidade vigentes.
- **Servidor Corporativo** – recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas de informação;
- **Software** – são todos os programas existentes em um computador, como sistema operacional, aplicativos, entre outros;
- **Site** – conjunto de páginas virtuais dinâmicas ou estáticas, que tem como principal objetivo fazer a divulgação da instituição;
- **Termo de Responsabilidade** – termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;
- **Tratamento de Incidentes de Segurança em Redes Computacionais** – serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair

informações que permitam impedir a continuidade da ação maliciosa e identificação de tendências;

- **Usuário** – servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Prefeitura Municipal de Itaguaí, formalizada por meio da assinatura do Termo de Responsabilidade;
- **Vulnerabilidade** – conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;

2) ÂMBITO DA POLÍTICA

2.1) As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores que exercem atividades no âmbito da administração pública direta e indireta na Prefeitura Municipal de Itaguaí, ou qualquer pessoa e ou empresa que venha a ter acesso a dados ou informações e em qualquer meio ou suporte.

2.2) Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da instituição poderão ser monitorados e gravados conforme previsto nas leis brasileiras.

2.3) É também obrigação de cada colaborador se manter atualizado em relação a esta PSIP e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da STI – Subsecretaria de Tecnologia da Informação, sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

3) DIRETRIZES GERAIS

3.1) A Política de Segurança da Informação e Privacidade será divulgada aos colaboradores, visando garantir que todos tenham consciência do seu conteúdo e a exerçam nas atividades relacionadas no âmbito da Prefeitura.

3.2) A responsabilidade pela Segurança da Informação e Privacidade deverá ser atribuída ao colaborador, quando da sua admissão na Prefeitura.

3.3) Deverão ser previstos, nos contratos de prestação de serviços de terceiros, cláusulas que contemplem as responsabilidades no cumprimento desta Política de Segurança da Informação e Privacidade, suas normas e procedimentos.

3.4) Os colaboradores são responsáveis pelo uso indevido, negligente ou imprudente dos recursos e serviços concedidos, bem como por qualquer prejuízo ou dano que vier a sofrer ou causar à Prefeitura ou a terceiros, em decorrência da não obediência às diretrizes e normas estabelecidas nessa política.

3.5) Todos os mecanismos de proteção utilizados para a segurança da informação e privacidade devem ser mantidos, a fim de preservar o princípio da continuidade nas atividades da Prefeitura.

3.6) Toda informação gerada pelos colaboradores, utilizando integralmente ou parcialmente recursos corporativos são de propriedade da Prefeitura Municipal de Itaguaí.

3.7) O Colaborador será responsável pela confidencialidade de qualquer senha que lhe tenha sido concedida para acesso ou uso da informação da Prefeitura, sendo a mesma de caráter pessoal e intransferível, não podendo ser compartilhada em nenhuma hipótese.

3.8) Quando a Informação, por meio de ativo de TI, for acessada externamente ao ambiente da Prefeitura, deverão ser observados os requisitos de segurança para a sua adequada proteção.

3.9) Ameaças e riscos devem ser reavaliados periodicamente para garantir que a Instituição esteja efetivamente protegida;

3.10) O acesso às informações, produzidas ou recebidas, devem ser limitadas às atribuições necessárias ao desempenho das respectivas atividades dos colaboradores.

3.11) Os processos de aquisição ou contratação de bens e serviços de tecnologia da informação, a qualquer título, devem refletir esta Política e demais normativas posteriores, sem prejuízo da observância da legislação em vigor.

3.12) Os equipamentos de tecnologia da informação, comunicação, sistemas e informações deverão ser utilizados exclusivamente para a realização das atividades profissionais. Os colaboradores devem evitar a circulação das informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito de “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

3.13) Um Plano de "Backup da Informação" deverá ser implementado e testado periodicamente, visando reduzir riscos de perda de disponibilidade e integridade de informação, por meio de ações de prevenção e recuperação.

4) CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do gestor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela de classificação a seguir:

- **Pública** – É toda informação que pode ser acessada por usuários da instituição, clientes, fornecedores, prestadores de serviços e público em geral.
- **Interna** – É toda informação que só pode ser acessada por funcionários da instituição. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.
- **Confidencial** – É toda informação que pode ser acessada por usuários da instituição e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.
- **Restrita** – É toda informação que pode ser acessada somente por usuários da instituição explicitamente indicado pelo nome ou por área a que pertence. A

divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da Instituição.

5) COMPETÊNCIAS E RESPONSABILIDADES

5.1) SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO – SMAD:

- Assegurar que a implementação dos controles de segurança da informação e privacidade tenha uma coordenação e permeie toda a instituição.
- Apoiar a Política e manter compromisso com sua continuidade e resultados.

5.2) SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO – STI:

- Promover acultura de segurança da informação e privacidade.
- Acompanhar as investigações e as avaliações dos danos decorrentes de possíveis incidentes de segurança.
- Propor recursos necessários às ações de segurança da informação e privacidade.
- Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e privacidade.
- Propor Normas Complementares e Procedimentos de Segurança da Informação e Privacidade.
- Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança da informação e privacidade.
- Apurar os incidentes de segurança críticos e encaminhar os fatos apurados para aplicação das penalidades previstas.
- Supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação e privacidade.
- Identificar e implementar controles físicos, administrativos e tecnológicos para a mitigação dos riscos.

- Recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança, informando aos respectivos gestores sobre as ações corretivas ou de contingência em cada caso.

5.3) Cabe aos Colaboradores da PREFEITURA MUNICIPAL DE ITAGUAÍ:

- Cumprir f fielmente com as determinações desta política, suas diretrizes e demais normas estabelecidas.
- Estar sempre atualizado e ciente das políticas, normas e procedimentos vigentes.
- Ser responsável pela confidencialidade de qualquer senha que lhe tenha sido concedida para acesso ou uso da informação da instituição, sendo a mesma de caráter pessoal e intransferível, não podendo ser compartilhada em nenhuma hipótese.
- Não divulgar, compartilhar ou transmitir informações a pessoas que não tenham nível de autorização suficiente.
- Não conduzir, transportar, enviar, transmitir, compartilhar ou deixar que dados e informações internas alcancem ambiente ou destinatário fora das dependências ou controle da instituição, sem autorização formal do gestor do setor proprietário/responsável pela da informação.

5.4) Cabe a Subsecretaria de Recursos Humanos da SMAD:

- Informar a STI – Subsecretaria de Tecnologia da Informação, todos os desligamentos, afastamentos, retornos e modificações no quadro funcional.

5.5) Cabe à Procuradoria Geral do Município – PGM:

- Prestar assessoramento de natureza jurídica, supervisionar e coordenar as atividades de natureza jurídica, inclusive aquelas relacionadas com a elaboração de atos normativos.

6) PENALIDADES

O descumprimento das disposições constantes nessa Política e nas demais normas sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, e dependendo da gravidade do caso, este poderá acarretar também em processo civil e penal.

7) CONSIDERAÇÕES FINAIS

Esta política de Segurança da Informação será complementada por normas e políticas inter-relacionadas que serão consideradas partes integrantes deste documento e serão detalhadas e divulgadas em documentos específicos, como, por exemplo, uso de correio eletrônico, da rede corporativa, da Internet, entre outros. Os casos omissos e dúvidas serão submetidos a Subsecretaria de Tecnologia da Informação.

Esta política será reavaliada, pelo menos, anualmente ou quando se julgar necessário, a critério da CDTSIP – Comissão Permanente de Diretrizes de Tecnologia, Segurança da Informação e Privacidade da Prefeitura Municipal de Itaguaí. A CDTSIP – Comissão Permanente de Diretrizes de Tecnologia, Segurança da Informação e Privacidade, órgão de deliberação coletiva, que será responsável pelos demais atos normativos vinculados a esta Política, e os seus membros serão nomeados pelo Chefe do Poder Executivo através de Portaria.