IV - Analistas de Vulnerabilidades e Hardening;

V - Analistas de Inteligência de Ameaças;

VI - Especialistas em Testes e Exercícios, quando aplicável.

§1º A composição nominal, inclusive substitutos, será definida por ato próprio da Presidência da ATI-TO, com indicação de responsabilidades e contatos funcionais.

§2º Poderão compor a atuação do NIRTI, por convocação, especialistas de outras áreas da ATI-TO e pontos focais de órgãos atendidos, conforme natureza do incidente ou atividade.

Art. 10. A implantação do NIRTI será progressiva e deverá observar um plano de trabalho a ser elaborado pelo Coordenador do NIRTI.

Art. 11. Os casos omissos serão dirimidos pela Presidência da ATI-TO, ouvida a Superintendência de Infraestrutura e Serviços de Tecnologia da Informação, bem como a Gerência de Segurança.

Art. 12. Esta Portaria entra em vigor na data de sua publicação.

Gabinete da Presidência da Agência de Tecnologia da Informação do Estado do Tocantins, em Palmas - TO, aos 02 dias do mês de março de 2026.

ALÍRIO FELIX MARTINS BARROS
Presidente da Agência de Tecnologia da Informação

PORTARIA Nº 28/2026/GABPRES/ATI, DE 02/03/2026.

Institui a Política de Segurança da Informação da Agência de Tecnologia da Informação do Estado do Tocantins.

O PRESIDENTE DA AGÊNCIA DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe foram conferidas pelo art. 42, §1º, incisos I e IV, da Constituição Estadual e da Lei 3.421, de 8 de março de 2019, e

CONSIDERANDO a competência da ATI-TO de elaborar, coordenar e executar a Política de Segurança da Informação dos órgãos e entidades da Administração Pública Direta e Indireta do Poder Executivo, consoante disposto no art. 7º, II, da Lei Estadual nº 3.421, de 8 de março de 2019, art. 14 do Decreto nº 6.547, de 13 de dezembro de 2022 e art. 1º, IV, do Regimento Interno da Agência de Tecnologia da Informação, publicado no DOE 6.568, de 10 de maio de 2024;

CONSIDERANDO a necessidade de estabelecer diretrizes que assegurem a proteção adequada das informações e ativos sob gestão desta Agência, assim como assegurar o cumprimento das melhores práticas de segurança da informação e conformidade com a legislação vigente,

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação da ATI-TO, que estabelece objetivos, princípios, diretrizes e responsabilidades relacionadas à Segurança da Informação.

Parágrafo único. Esta política se aplica a todos os ativos de informação administrados, mantidos ou utilizados pela Agência, incluindo dados, sistemas, redes e infraestrutura física, bem como a todos os usuários de Tecnologia da Informação que acessam ou processam informações custodiadas pela ATI-TO.

CAPÍTULO I
Das Disposições Preliminares

Art. 2º A Política de Segurança da Informação é uma declaração de compromisso desta instituição com a proteção das informações que cria, manipula, custodia ou que são de sua propriedade, sob o gerenciamento de sua infraestrutura de TI, devendo ser conhecida, compreendida e cumprida por todos que tenham acesso a estas informações.

Parágrafo único. A utilização dos recursos de TI da Agência ou de recursos particulares em seu proveito deve ser pautada pelos princípios da ética, segurança e legalidade.

Seção I
Da Organização, Aprovação e Atualização Normativa

Art. 3º A Política da Segurança da Informação da ATI-TO compreende:

I - Diretrizes gerais e princípios básicos com a finalidade de nortear todas as ações, visando garantir a manutenção da Segurança da Informação;

II - Normas de Segurança da Informação que estabelecem os controles, métodos, restrições e responsabilidades para atendimento à PSI atinentes a temáticas específicas aplicadas ao nível de acesso dos usuários de recursos tecnológicos e sistemas de informações da Agência;

Parágrafo único. Caberá às superintendências da ATI-TO zelar pela ciência, publicidade e cumprimento das normativas vinculadas à sua área de atuação por parte de seus respectivos usuários;

III - Procedimentos de Segurança da Informação que definem como as operações de atendimento à PSI e normas correlatas devem ser realizadas.

§1º Além destes procedimentos também compõem a Política da Segurança da Informação outros documentos acessórios, tais como: termos e acordos de uso/responsabilidade e confidencialidade perante quem tomar contato com informações custodiadas e/ou de propriedade da ATI-TO.

§2º As revisões da Política, das normas e procedimentos ocorrerão conforme a necessidade, sendo aprovadas diretamente pela presidência da Agência.

Seção II
Das Definições

Art. 4º Para fins desta Política, consideram-se as seguintes definições principais:

I - Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

II - Ativos de Informação: qualquer elemento (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio e que tenha valor para a ATI-TO e precisa ser adequadamente protegido. Inclui 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 têm acesso;

III - Gestor da Segurança da Informação: responsável pelas ações de segurança da informação no âmbito da ATI-TO, coordenando o Comitê de Segurança da Informação (CSI) e a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR);

IV - Incidente de Segurança da Informação: ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede que indica possível violação à Política de Segurança ou Normas complementares, falha de controles ou situação previamente desconhecida e que possa ser relevante à segurança da informação.

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

VI - Segurança da Informação: conjunto de práticas e processos que visam proteger informações e sistemas contra acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados;

VII - Tratamento da Informação: conjunto de ações e controles que, aplicados, visam proteger as informações durante todo o seu ciclo de vida independentemente do meio (físico ou lógico).

VIII - Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

IX - Agente Público ou Usuário de Informação: Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Estadual, direta e indireta.

Seção III
Dos Objetivos

Art. 5º São objetivos desta Política:

I - declarar formalmente o comprometimento da ATI-TO na definição de diretrizes estratégicas, responsabilidades, competências e apoio ao Sistema de Gestão de Segurança da Informação (SGSI), a fim de garantir a proteção dos seus ativos tangíveis e intangíveis;

II - estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações;

III - estabelecer competências e responsabilidades quanto à segurança da informação;

IV - nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação na ATI-TO;

V - promover o alinhamento das ações de segurança da informação com as estratégias de planejamento organizacional da ATI-TO.

CAPÍTULO II
Dos Princípios e Diretrizes

Seção I
Dos Princípios

Art. 6º A Segurança da Informação da ATI-TO observará os seguintes princípios:

a) Auditabilidade: visa permitir o rastreio de todas as transações ou eventos relacionados à informação, de forma a detectar alterações ou acessos indevidos por parte das auditorias internas ou externas, assegurando que todas as ações realizadas foram devidamente autorizadas e estão em conformidade com as políticas de segurança estabelecidas.

b) Autenticidade: assegurar que a informação seja proveniente da fonte anunciada e que não tenha sofrido alterações ao longo do processo;

c) Confidencialidade: garantir que as informações sejam acessíveis apenas àqueles autorizados a ter acesso;

d) Disponibilidade: garantir que as informações estejam acessíveis aos usuários autorizados sempre que necessário;

e) Integridade: assegurar a completude e precisão das informações e métodos de processamento;

f) Legalidade: visa assegurar o cumprimento de Leis, regulamentos, políticas e normas éticas aplicáveis ao tratamento de dados e informações em todas as fases de seu ciclo de vida, de modo transparente e ético, visando coibir qualquer ato que envolva desvio de conduta de pessoas a serviço da Administração, sob a forma de corrupção, fraude, suborno, favorecimento ilícito, extorsão, entre outros.

g) Não Repúdio: visa assegurar que, uma vez realizada uma ação ou comunicado um dado, o autor não possa negar sua autoria ou envio, garantindo que as partes envolvidas não possam contestar a autenticidade de suas ações.

h) Privacidade: garantir a proteção dos dados pessoais e o respeito à privacidade dos indivíduos;

i) Proteção: salvaguardar as informações contra acessos, modificações, destruições ou divulgações não autorizadas;

j) Responsabilidade: definir claramente as responsabilidades pela segurança da informação e utilizar as informações de maneira ética e responsável.

Seção II
Das Diretrizes

Art. 7º São diretrizes da Segurança da Informação na ATI-TO, organizadas conforme as categorias da ISO/IEC 27002:

I - Controles Organizacionais: Implementar políticas e procedimentos de segurança da informação.

II - Controles de Acesso: Implementar controles de acesso baseados no princípio do menor privilégio.

III - Controles Criptográficos: Utilizar criptografia para proteger informações sensíveis.

IV - Controles Físicos e Ambientais: Implementar controles de segurança física para proteger instalações e equipamentos.

V - Controles de Operações: Estabelecer procedimentos de backup e recuperação de dados.

VI - Controles de Comunicações: Implementar controles de segurança de rede, incluindo firewalls e sistemas de detecção de intrusões.

VII - Controles de Aquisição e Desenvolvimento: Implementar controles de segurança para desenvolvimento e aquisição de sistemas.

VIII - Controles de Gestão de Incidentes: Estabelecer processos de gestão de incidentes de segurança da informação.

IX - Controles de Conformidade: Implementar controles de segurança para garantir a conformidade com requisitos legais e regulatórios.

Art. 8º A Política de Segurança da Informação e demais instruções normativas dela derivadas fazem parte do conjunto de regras que orientam o Sistema de Gestão de Segurança da Informação da ATI-TO.

Parágrafo único: O Sistema de Gestão de Segurança da Informação (SGSI) da ATI-TO terá como escopo a proteção de todos os ativos de informação sob sua responsabilidade, incluindo dados, sistemas, redes e infraestrutura física, em conformidade com os requisitos da ISO/IEC 27001.

CAPÍTULO III
Das Ações de Segurança da Informação

Art. 9º As ações de segurança da informação devem:

a) ser tratadas de forma integrada, respeitando as especificidades e a autonomia das superintendências dispostas no organograma da ATI-TO;

b) ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação;

c) visar à prevenção da ocorrência de incidentes de segurança.

Art. 10. Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada pela ATI-TO compõe o seu rol de ativos de informação e deve ser protegida conforme as normas em vigor.

Parágrafo único. As informações citadas no *caput*, que trafegam pelo ambiente computacional e/ou em equipamentos de TI sob a gestão da ATI-TO, são passíveis de monitoramento e auditoria pela Agência, respeitados os limites legais.

Art. 11. Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

Parágrafo único. O acesso aos recursos de tecnologia da informação da ATI-TO está condicionado à assinatura, preferencialmente por meio eletrônico, de Termo de Responsabilidade, no qual o usuário deve declarar que tomou conhecimento dos termos desta Política, das responsabilidades e compromissos decorrentes desse acesso, bem como das penalidades aplicáveis pela inobservância das normas de segurança da informação.

Art. 12. A Política de Segurança da Informação e suas atualizações, bem como normas específicas de segurança da informação da Agência, devem ser divulgadas amplamente a todos os Usuários de Informação, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

§1º Os Usuários de Informação devem ser continuamente capacitados nos procedimentos de segurança e no uso correto dos ativos de informação quando da realização de suas atribuições, de modo a minimizar possíveis riscos à segurança da informação.

§2º As ações de capacitação previstas no §1º devem ser conduzidas de modo a possibilitar o compartilhamento de materiais educacionais sobre segurança da informação.

Art. 13. Todos os contratos de prestação de serviços firmados pela ATI-TO deverão conter cláusula específica sobre a obrigatoriedade de atendimento a esta Política de Segurança da Informação e às suas normas decorrentes nos itens aplicáveis.

CAPÍTULO IV
Da Gestão da Segurança da Informação

Seção I
Da Estrutura de GSI

Art. 14. A estrutura de Gestão de Segurança da Informação da ATI-TO compreende:

I - Administração Superior;

II - Comitê de Segurança da Informação;

III - Gestor de Segurança da Informação;

IV - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR);

V - Encarregado pelo Tratamento de Dados Pessoais;

VI - Escritório de Governança de Dados;

VII - Usuários de informação.

Seção II
Das Responsabilidades

Art. 15. Compete à Administração Superior da ATI-TO:

I - Aprovar a Política de Segurança da Informação e suas revisões;

II - Prover os recursos necessários para a implementação e manutenção do Sistema de Gestão de Segurança da Informação;

III - Incentivar e apoiar a disseminação de boas práticas de segurança da informação entre os usuários da informação da Agência;

IV - Assegurar o alinhamento da Política de Segurança da Informação e de suas normas derivadas ao Planejamento Estratégico da ATI-TO.

Art. 16. Compete ao Comitê de Segurança da Informação:

I - Propor e revisar a Política de Segurança da Informação;

II - Aprovar normas e procedimentos de Segurança da Informação;

III - Avaliar e priorizar projetos e iniciativas de Segurança da Informação;

IV - Analisar os resultados das avaliações de risco e auditorias de segurança;

V - Deliberar sobre questões estratégicas de Segurança da Informação.

Art. 17. Compete ao Gestor da Segurança da Informação:

I - Coordenar a implementação e manutenção do Sistema de Gestão de Segurança da Informação;

II - Elaborar e manter atualizadas as normas e procedimentos de Segurança da Informação;

III - Coordenar as avaliações de risco de Segurança da Informação;

IV - Monitorar e reportar o status da Segurança da Informação para a administração superior;

V - Coordenar o programa de conscientização em segurança da informação;

VI - Gerenciar a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR);

VII - Atuar como ponto focal para questões de segurança da informação.

Art. 18. Compete à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR):

I - Receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança;

II - Realizar a triagem de incidentes de segurança e coordenar a resposta apropriada;

III - Realizar análises forenses de incidentes de segurança, quando necessário;

IV - Manter um registro de incidentes de segurança e lições aprendidas;

V - Propor melhorias nos controles de segurança com base na análise de incidentes.

Art. 19. Compete ao Encarregado pelo Tratamento de Dados Pessoais:

I - Colaborar com o Gestor de Segurança da Informação na identificação, avaliação e tratamento dos riscos de segurança relacionados ao tratamento de dados pessoais;

II - Assegurar que as medidas de segurança implementadas estejam em conformidade com a Lei Geral de Proteção de Dados Pessoais - LGPD e outras regulamentações de proteção de dados aplicáveis;

III - Participar na elaboração e revisão de políticas, procedimentos e diretrizes de segurança que impactem o tratamento de dados pessoais;

IV - Manter-se atualizado sobre as melhores práticas de segurança da informação relacionadas à proteção de dados pessoais.

Art. 20. Compete ao Escritório de Governança de Dados:

I - Colaborar com a área de Segurança da Informação na definição e implementação de políticas e procedimentos de classificação e proteção de dados, garantindo que os requisitos de segurança sejam adequados à sensibilidade e criticidade dos dados;

II - Apoiar a identificação e mapeamento de fluxos de dados críticos, auxiliando na priorização de esforços de segurança da informação;

III - Trabalhar em conjunto com a equipe de Segurança da Informação para garantir que os controles de acesso aos dados estejam alinhados com os princípios de governança de dados, como o princípio do menor privilégio;

IV - Auxiliar na resposta a incidentes de segurança relacionados a dados, fornecendo informações sobre a natureza, sensibilidade e impacto potencial dos dados afetados.

Art. 21. Compete aos Agentes Públicos ou Usuários de Informação:

I - Cumprir esta Política de Segurança da Informação e as normas e procedimentos dela derivados;

II - Proteger as informações e ativos de TI sob sua responsabilidade;

III - Reportar incidentes e vulnerabilidades de segurança;

IV - Participar dos treinamentos de conscientização em segurança da informação.

Art. 22. Para fins desta Política, o Comitê de Segurança da Informação será composto pelo Gestor de Segurança da Informação e pelos membros do Comitê de Gestão da ATI.

CAPÍTULO V
Da Gestão de Riscos de Segurança da Informação

Art. 23. A gestão de riscos de segurança da informação na ATI-TO deve estar alinhada ao modelo de gestão de riscos institucional, compatível com a missão e os objetivos estratégicos da Agência, considerando:

I. os processos internos institucionais;

II. os requisitos legais aplicáveis;

III. a Política de Segurança da Informação da ATI-TO;

IV. a Política de Gestão de Riscos institucional, e

V. a estrutura organizacional da ATI-TO.

Art. 24. O processo de gestão de riscos de segurança da informação tem por objetivo direcionar e controlar os riscos, a fim de adequá-los aos níveis aceitáveis para a ATI-TO.

Art. 25. O processo de gestão de riscos de segurança da informação deverá fornecer os seguintes documentos:

I - Plano de Gestão de Riscos de Segurança da Informação;

II - Relatório de Identificação, Análise e Avaliação dos Riscos de Segurança da Informação; e

III - Relatório de Tratamento de Riscos de Segurança da Informação.

CAPÍTULO VI
Da Gestão de Ativos de Informação

Art. 26. Todos os ativos de informação da ATI-TO devem ser identificados, classificados e ter responsáveis designados para sua gestão.

Art. 27. Os ativos de informação devem ser protegidos contra acessos não autorizados, danos ou perdas, de acordo com sua classificação e criticidade.

Art. 28. O descarte ou reutilização de ativos de informação deve ser realizado de forma segura, garantindo a eliminação completa de dados sensíveis ou confidenciais.

CAPÍTULO VII
Do Controle de Acesso

Art. 29. O acesso às informações e sistemas da ATI-TO será concedido com base no princípio do menor privilégio, garantindo que os usuários tenham apenas as permissões necessárias para o desempenho de suas funções.

Art. 30. Os mecanismos de autenticação e autorização devem ser implementados para assegurar que apenas usuários autorizados tenham acesso aos recursos da ATI-TO.

Art. 31. É proibido o compartilhamento de credenciais de acesso entre usuários. Cada usuário é responsável pelo uso adequado de suas credenciais.

CAPÍTULO VIII
Da Gestão de Incidentes de Segurança da Informação

Art. 32. A ATI-TO deve estabelecer e manter procedimentos para a identificação, registro, análise e resposta a incidentes de segurança da informação.

Art. 33. Todos os usuários têm a responsabilidade de reportar imediatamente quaisquer incidentes ou suspeitas de incidentes de segurança da informação ao Gestor de Segurança da Informação ou à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

Art. 34. Os incidentes de segurança da informação devem ser documentados e analisados para identificar causas raiz e implementar medidas corretivas e preventivas.

CAPÍTULO IX
Da Conscientização e Capacitação em Segurança da Informação

Art. 35. A ATI-TO deve promover programas contínuos de conscientização e treinamento em segurança da informação para todos os usuários, visando ao fortalecimento da cultura de segurança e à mitigação de riscos associados ao comportamento humano.

Art. 36. Os treinamentos devem ser adequados às funções e responsabilidades dos usuários, garantindo que todos compreendam suas obrigações em relação à segurança da informação.

CAPÍTULO X
Das Violações e Sanções

Art. 37. O não cumprimento desta Política e das normas de segurança da informação dela derivadas estará sujeito às sanções previstas na Lei nº 1.818, de 23 de agosto de 2007 - Estatuto dos Servidores Públicos Civis do Estado do Tocantins, sem prejuízo das demais medidas administrativas, cíveis e penais cabíveis.

Parágrafo único. A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

CAPÍTULO XI
Das Vedações e Disposições Finais

Art. 38. É vedada a utilização dos ativos de tecnologia da informação disponibilizados pela ATI-TO para acesso, guarda e divulgação de material incompatível com o ambiente de trabalho, que viole direitos autorais ou que infrinja a legislação vigente.

Art. 39. São vedados o uso e a instalação dos ativos de tecnologia da informação não homologados, licenciados ou adquiridos pelo Governo do Estado do Tocantins, salvo autorização expressa da Administração Superior da ATI-TO.

Art. 40. É vedada a instalação de softwares de qualquer natureza nos ativos de TI de propriedade ou de posse da Agência de Tecnologia da Informação, sem autorização do setor responsável.

Art. 41. É vedada a divulgação e/ou compartilhamento com terceiros dos mecanismos de identificação, autenticação e autorização baseados em conta e senha ou certificação digital, de uso pessoal e intransferível, que são fornecidos aos usuários pela ATI-TO.

Art. 42. As unidades organizacionais da ATI-TO devem promover ações de treinamento e conscientização para que os seus usuários entendam suas responsabilidades e procedimentos voltados à segurança da informação e à proteção de dados.

Parágrafo único. A conscientização, a capacitação e a sensibilização em segurança da informação devem ser adequadas aos papéis e responsabilidades dos usuários.

Art. 43. As denúncias de violação a esta Política podem ser comunicadas ao Gestor de Segurança da Informação e feitas através dos seguintes canais: e-mail, telefone corporativo, central de serviços ou ouvidoria.

Art. 44. O cumprimento desta Política, bem como dos normativos e procedimentos acessórios que a complementam devem ser avaliados por Grupo de Trabalho multidisciplinar instituído pela Comissão de Segurança da Informação periodicamente para realizar verificações de conformidade, buscando a certificação do cumprimento dos requisitos de segurança da informação e da garantia de cláusula de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos similares.

Art. 45. Casos omissos ou esclarecimentos desta Política, Normas Complementares ou Procedimentos da ATI-TO são de responsabilidade do Comitê de Segurança da Informação (CSI) e passíveis de aprovação pela Presidência da Agência.

Art. 46. Esta Portaria entra em vigor na data de sua publicação.

ALÍRIO FELIX MARTINS BARROS
Presidente da Agência de Tecnologia da Informação

INSTRUÇÃO NORMATIVA ATI Nº 1/2026/GABPRES, DE 02/03/2026.

Institui a Política de Governança de Dados no âmbito da Agência de Tecnologia da Informação do Estado do Tocantins.

O PRESIDENTE DA AGÊNCIA DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe foram conferidas pelo art. 42, §1º, incisos I e IV, da Constituição Estadual, c/c o art. 10, parágrafo único, da Lei 3.421, de 8 de março de 2019 e

CONSIDERANDO as competências da Agência de Tecnologia da Informação do Estado do Tocantins - ATI-TO, dispostas no artigo 7º, da Lei nº 3.421, de 08 de março de 2019, especialmente no que tange à gestão de dados governamentais, bem como os regramentos trazidos pelo Decreto nº 6.547, de 13 de dezembro de 2022, que regulamenta a aplicação da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) no âmbito da Administração Pública do Estado do Tocantins;

CONSIDERANDO os parâmetros norteadores para a governança e compartilhamento de dados elencados no Decreto Federal nº 10.046, de 09 de outubro de 2019;

CONSIDERANDO a necessidade de estabelecer diretrizes para a governança de dados que assegurem a qualidade, integridade, segurança e eficácia no uso dos dados governamentais;

CONSIDERANDO as normas técnicas e as melhores práticas nacionais e internacionais para a governança de dados, incluindo o Modelo de Maturidade de Dados da Administração Pública Federal - MMD, o Guia de Conhecimento em Gerenciamento de Dados - DMBOK e os Objetivos de Controle para Informação e Tecnologia Relacionada - COBIT;

RESOLVE:

Art. 1º Instituir a Política de Governança de Dados da Agência de Tecnologia da Informação do Estado do Tocantins, com o objetivo de estabelecer princípios, diretrizes e responsabilidades para o gerenciamento eficaz dos dados institucionais e administração dos dados governamentais.

Parágrafo único. Esta política se aplica a todos os dados gerados, coletados, armazenados, processados ou transmitidos pela instituição, em qualquer formato ou meio, incluindo dados estruturados e não estruturados, internos e externos no que couber.

Art. 2º Para os fins desta Instrução Normativa, consideram-se as seguintes definições:

I - Governança de Dados: conjunto de processos, papéis, políticas, padrões e métricas que garantem o uso eficaz e eficiente dos dados;

II - Dados: representações de fatos, conceitos ou instruções de forma adequada para comunicação, interpretação ou processamento por seres humanos ou por meios automáticos;

III - Informação: dado contextualizado;

IV - Metadados: dados que descrevem outros dados, fornecendo contexto e significado;

V - Catálogo de Dados: repositório centralizado que armazena metadados sobre os dados;

VI - Dados mestres: são dados de referência, cadastrais e essenciais para caracterizar as entidades fundamentais para a instituição, como os cidadãos, os servidores, os bens patrimoniais, os serviços públicos e outros;

VII - Ciclo de Vida dos Dados: sequência de estágios pelos quais os dados passam, desde sua obtenção ou criação até seu arquivamento ou eliminação;

VIII - Arquitetura de Dados: estrutura que define como os dados são coletados, armazenados, transformados, distribuídos e consumidos dentro da organização;

IX - Qualidade de Dados: grau em que os dados atendem às necessidades e expectativas dos usuários em termos de acurácia, completude, consistência e atualidade;

X - Ativo de dados: qualquer informação ou conjunto de informações que pode gerar valor para a instituição quando gerenciado de forma eficaz;

XI - Comitê de Governança de Dados: órgão colegiado responsável por definir estratégias, aprovar políticas, definir prioridades e investimentos em governança de dados e supervisionar sua implementação;

XII - Escritório de Governança de Dados: unidade responsável pela coordenação e execução das atividades de governança de dados;

XIII - Executivos de Dados: pessoas designadas para comporem o Comitê de Governança de Dados, responsáveis por definir a visão e a estratégia em relação aos dados, garantindo que a governança de dados esteja alinhada com os objetivos estratégicos da agência;

XIV - Gestores de Dados: liderança máxima das unidades, responsáveis pela qualidade, integridade, uso adequado e proteção dos dados em sua área de atuação;

XV - Curadores de Dados: servidores designados como responsáveis pela gestão técnica de um conjunto específico de dados, incluindo o design, a implementação e a manutenção das bases de dados;

XVI - Usuários de dados: todos os servidores e colaboradores que utilizam dados em suas atividades;

XVII - Dicionário de Dados: documento que contém metadados sobre a estrutura, formato e uso de dados em um sistema ou base de dados;

XVIII - Gestão de Dados: prática de garantir que os ativos de dados de alta qualidade estejam disponíveis para atender às necessidades da organização;