I - ABIANE CARVALHO FREITAS, Matrícula nº 1273132-1
II - AGNES ROCHA BARBOSA, Matrícula nº 11217120-1
III - APARECIDA MARIA DE JESUS, Matrícula nº 868775-1
IV - LUCIANA CASTRO DE SABOIA OLIVEIRA, Matrícula nº 1289110-1

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

PUBLIQUE-SE, REGISTRE-SE E CUMPRA-SE.

GABINETE DA PRESIDÊNCIA DA AGÊNCIA DE METROLOGIA, AVALIAÇÃO DA CONFORMIDADE, INOVAÇÃO E TECNOLOGIA DO ESTADO DO TOCANTINS (AEM/TO), Órgão Delegado do INMETRO, em Palmas, Capital do Estado do Tocantins, aos 02 dias do mês de março do ano de 2026.

DENNER GLEIK ROSA MARTINS
Presidente

AGETO

EXTRATO DO 2º TERMO ADITIVO AO CONTRATO Nº 009/2025

PROCESSO Nº: 2024/38960/004055
CONTRATO Nº: 009/2025
CONTRATANTE: AGÊNCIA DE TRANSPORTES, OBRAS E INFRAESTRUTURA - AGETO
CONTRATADA: CONSORCIO RODOVIAS DO TOCANTINS
CPF/CNPJ: 59.004.649/0001-23
OBJETO: A PRORROGAÇÃO DO PRAZO DE VIGÊNCIA CONTRATUAL POR MAIS 12 (DOZE) MESES (RENOVAÇÃO), BEM COMO A SUPRESSÃO DE QUANTITATIVOS NÃO REMANESCENTES DO PERÍODO ANTERIOR, RELATIVA AO CONTRATO ADMINISTRATIVO Nº 009/2025, CUJO OBJETO CONSISTE NA CONTRATAÇÃO DE EMPRESA PARA A EXECUÇÃO DE SERVIÇOS CONTÍNUOS DE CONSERVAÇÃO RODOVIÁRIA, COMPREENDENDO OPERAÇÕES ROTINEIRAS, PREVENTIVAS PERIÓDICAS, CORRETIVAS E ESPECIAIS NAS RODOVIAS, OBRAS DE ARTE ESPECIAIS E AERÓDROMOS DO ESTADO DO TOCANTINS. LOTE 12 - REGIÃO DE CONSERVAÇÃO 12 - CIDADE POLO PEIXES.
PRAZO: 12 (doze) meses
VALOR: R$ 19.973.887,63 (dezenove milhões, novecentos e setenta e três mil, oitocentos e oitenta e sete reais e sessenta e três centavos)
FIRMADO EM: 27/02/2026
SIGNATÁRIOS: TÚLIO PARREIRA LABRE - Representante Legal da Contratante e FÁBIO CESAR COSTA - Representante Legal da Contratada

ATI

PORTARIA ATI Nº 27/2026/GABPRES/ATI, DE 02 DE MARÇO DE 2026.

Dispõe sobre a criação do Núcleo de Inteligência e Resiliência de Tecnologia da Informação - NIRTI

O PRESIDENTE DA AGÊNCIA DE TECNOLOGIA DA INFORMAÇÃO DO ESTADO DO TOCANTINS - ATI-TO, no uso de suas atribuições legais previstas na Lei Estadual nº 3.421, de 8 de março de 2019, e alterações, bem como no Regimento Interno da ATI-TO, e

CONSIDERANDO a competência da ATI-TO para elaborar, coordenar e executar a Política Estadual de Tecnologia da Informação e a Política de Segurança da Informação dos órgãos e entidades da Administração Pública Direta e Indireta do Poder Executivo Estadual, nos termos do art. 14 do Decreto nº 6.547, de 13 de dezembro de 2022;

CONSIDERANDO que o Regimento Interno da ATI-TO atribui à Gerência de Segurança atividades de monitoramento ativo com foco em segurança, análise de riscos, plano de continuidade e operacionalização de grupo de tratamento de incidentes;

CONSIDERANDO a necessidade de fortalecer a segurança e a continuidade dos serviços digitais do Tocantins, com capacidade permanente de proteção, detecção, resposta, recuperação e inteligência;

CONSIDERANDO os deveres legais e regulatórios referentes à proteção de dados pessoais, inclusive quanto à gestão e comunicação de incidentes de segurança que possam acarretar risco ou dano relevante, na forma da Lei Federal nº 13.709, de 14 de agosto de 2018 - LGPD e da Resolução CD/ANPD nº 15, de 24 de abril de 2024;

CONSIDERANDO a Política Estadual de Transformação para o Governo Digital (Decreto nº 6.757, de 5 de março de 2024) e a necessidade de segurança e resiliência como requisitos estruturantes para serviços públicos digitais;

RESOLVE:

Art. 1º Fica criado, no âmbito da ATI-TO, o Núcleo de Inteligência e Resiliência de Tecnologia da Informação - NIRTI, como unidade operacional especializada, vinculada à Superintendência de Infraestrutura e Serviços de Tecnologia da Informação, por meio da Diretoria de Infraestrutura e da Gerência de Segurança, com a finalidade de estruturar, coordenar e executar atividades de segurança e resiliência digital no escopo definido nesta Portaria.

§1º O NIRTI atuará de forma integrada com as demais unidades da ATI-TO, com os órgãos e entidades atendidos, e com as instâncias de governança e gestão de riscos aplicáveis, observadas as competências formais de cada unidade.

§2º O NIRTI não substitui as obrigações e responsabilidades dos órgãos e entidades estaduais quanto à gestão de seus riscos, ativos e dados e constitui capacidade central de apoio técnico e coordenação, no âmbito de serviços e infraestruturas sob gestão, operação ou hospedagem da ATI-TO, e nos demais casos em que houver instrumento formal de atendimento.

Art. 2º São finalidades do NIRTI:

I - realizar monitoramento contínuo, centralizado e proativo dos ambientes e ativos de TI sob responsabilidade da ATI-TO, visando detecção precoce de ameaças e resposta tempestiva;

II - detectar, analisar, coordenar e responder a incidentes de segurança cibernética no escopo das atividades da ATI-TO, promovendo contenção, erradicação e recuperação segura, com registro e evidências auditáveis;

III - operar processo contínuo de gestão de vulnerabilidades, incluindo identificação, priorização por risco, recomendação, acompanhamento e validação de correções - patching e medidas de fortalecimento -hardening;

IV - produzir e difundir inteligência de ameaças aplicável ao contexto do Estado do Tocantins, incluindo alertas técnicos e estratégicos;

V - planejar e conduzir simulações, exercícios e testes de segurança autorizados, visando melhoria de prontidão, detecção e resposta;

VI - fortalecer a resiliência cibernética e a continuidade dos serviços digitais, promovendo integração entre segurança, continuidade, recuperação e gestão de mudanças;

VII - medir e elevar a maturidade do programa de segurança cibernética no escopo de atuação, por meio de indicadores, metas e planos de melhoria contínua;

VIII - estabelecer, em conjunto com as áreas técnicas competentes, requisitos mínimos de segurança para homologação e entrada em produção de sistemas e mudanças relevantes, incluindo testes e evidências, conforme processos internos de gestão de mudanças.

Art. 3º O NIRTI atuará em regime contínuo, observando portfólio mínimo de serviços:

I - Monitoramento e Detecção - gestão de fontes de logs e sensores, correlação de eventos, detecção de comportamento anômalo, produção e ajuste de regras de detecção, utilizando as ferramentas disponíveis na ATI;

II - Resposta a Incidentes - triagem, classificação, investigação técnica, contenção, erradicação, recuperação e pós-incidente;

III - Gestão de Vulnerabilidades e Exposição - varreduras, controle de conformidade técnica, priorização baseada em risco e evidência de exploração, recomendações e validações;

IV - Inteligência de Ameaças coleta, análise, contextualização, alertas, indicadores de comprometimento -IOCs e recomendações acionáveis;

V - Avaliações de Segurança, Simulações e Exercícios - testes autorizados, exercícios de mesa e técnicos, e apoio a capacitação;

VI - Resiliência e Continuidade Cibernética - apoio técnico à definição e teste de procedimentos de recuperação, contingência e requisitos de disponibilidade para serviços críticos.

Parágrafo único. O detalhamento do portfólio, níveis de serviço, horários de cobertura, fluxos e critérios técnicos deverá constar em Norma Operacional do NIRTI, aprovada pela Superintendência de Infraestrutura e Serviços de Tecnologia da Informação.

Art. 4º São competências do NIRTI:

I - Estabelecer e operar mecanismos de monitoramento contínuo de eventos, tráfego e atividades suspeitas, com indicadores e trilhas de auditoria;

II - instituir e manter procedimentos operacionais padrão (POPs) e playbooks de resposta a incidentes, incluindo matriz de severidade, níveis de escalonamento e critérios de encerramento;

III - coordenar a resposta a incidentes no escopo, assegurando registro formal, rastreabilidade, preservação de evidências e relatório de lições aprendidas;

IV - gerenciar o ciclo de vulnerabilidades, correlacionando achados com inventário de ativos e criticidade de serviços, e conduzindo validações de correção;

V - emitir recomendações técnicas de hardening, segmentação, controle de acesso, backup, logging e demais controles prioritários, acompanhando sua execução;

VI - apoiar tecnicamente a gestão de incidentes envolvendo dados pessoais, fornecendo subsídios para decisões e comunicações, observado o papel do controlador e do encarregado competente;

VII - planejar e executar, quando autorizado, testes técnicos de segurança e exercícios de resposta, com evidências e relatórios;

VIII - produzir relatórios operacionais e gerenciais periódicos, com métricas de desempenho, tendências e riscos prioritários;

IX - propor plano anual de evolução de capacidades do NIRTI, com metas, indicadores, capacitação e investimentos prioritários.

Art. 5º A gestão de incidentes no âmbito do NIRTI deverá assegurar execução coordenada, documentada e auditável, contemplando, no mínimo, as fases:

I - Detecção, triagem e confirmação;

II - Contenção imediata e contenção estruturada;

III - Erradicação e correção de causa raiz;

IV - Recuperação e retorno seguro à operação;

V - Pós-incidente: relatório, lições aprendidas, plano de remediação e atualização de controles.

§1º Todo incidente deverá ser registrado em sistema oficial, com data/hora, origem do alerta, ativos afetados, classificação de severidade, responsáveis e evidências associadas.

§2º A preservação de evidências digitais deverá observar rastreabilidade e integridade (cadeia de custódia), compatível com auditoria e eventual apuração administrativa ou criminal.

§3º Incidentes com potencial impacto em dados pessoais deverão ser imediatamente comunicados, pelo rito definido em norma interna do Poder Executivo Estadual, às instâncias competentes de proteção de dados e governança, para avaliação de risco, dano relevante e providências cabíveis.

Art. 6º O processo de gestão de vulnerabilidades do NIRTI deverá:

I - manter inventário de ativos sob escopo, ou referência a inventário corporativo oficial, com classificação de criticidade;

II - realizar varreduras periódicas e extraordinárias, sempre que houver mudanças relevantes ou alertas críticos;

III - priorizar correções por risco, criticidade de serviço e evidência de exploração, com prazos recomendados;

IV - acompanhar a implementação das correções e validar sua efetividade;

V - manter registro histórico de vulnerabilidades, prazos e status de remediação, para fins de governança e auditoria.

Art. 7º O NIRTI instituirá processo de “segurança pré-produção” para sistemas e mudanças relevantes no escopo da ATI-TO, exigindo, conforme criticidade:

I - evidências mínimas de testes de segurança - incluindo varredura de vulnerabilidades e correção de não conformidades críticas antes de produção;

II - avaliação de risco e aprovação formal das áreas técnicas responsáveis e de segurança, conforme política interna de mudanças;

III - requisitos mínimos de logging e rastreabilidade compatíveis com monitoramento e investigação.

Art. 8º O NIRTI observará princípios de minimização, necessidade e confidencialidade no tratamento de informações e dados, adotando salvaguardas proporcionais ao risco, incluindo:

I - controle de acesso por perfil e segregação de funções;

II - registro e auditoria de ações administrativas e operacionais relevantes;

III - retenção e descarte de dados e evidências conforme norma interna, com justificativa e trilha de auditoria;

IV - anonimização ou pseudonimização quando tecnicamente viável, especialmente em relatórios gerenciais;

V - classificação de documentos e informações do NIRTI como “Acesso Restrito”, quando envolverem detalhes de vulnerabilidades, telemetria, investigações ou indicadores sensíveis.

Art. 9º A estrutura funcional mínima do NIRTI compreenderá:

I - Coordenador do NIRTI, preferencialmente exercido pelo titular da Gerência de Segurança ou por designação formal da Presidência, responsável por planejamento, priorização, indicadores, escalonamentos e reporte executivo;

II - Analistas de Monitoramento e Detecção;

III - Analistas/Especialistas de Resposta a Incidentes;

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).