

ATI

**INSTRUÇÃO NORMATIVA Nº 2/2026/GABPRES/ATI,
DE 01/04/2026.**

Estabelece as regras de controle de acesso e os requisitos de segurança para serviços digitais no âmbito da Agência de Tecnologia da Informação do Estado do Tocantins - ATI/TO.

O PRESIDENTE DA ATI/TO, no uso das atribuições que lhe confere o art. 42, §1º, incisos I e IV, da Constituição Estadual, a Lei nº 3.421 de 08 de março de 2019, o Decreto Estadual nº 6.547, de 13 de dezembro de 2022 e a Portaria ATI/TO nº 28, de 02 de março de 2026,

CONSIDERANDO que o acesso indevido a sistemas e dados é uma das principais causas de incidentes de segurança na administração pública;

CONSIDERANDO que os serviços digitais ofertados ao cidadão exigem padrões mínimos de autenticação, proteção de dados e rastreabilidade;

CONSIDERANDO que o princípio do menor privilégio é fundamental para reduzir a superfície de ataque e proteger dados pessoais e informações sensíveis;

CONSIDERANDO que a rastreabilidade dos acessos é requisito essencial de governança, auditoria e conformidade com a Lei Geral De Proteção de Dados Pessoais - LGPD,

RESOLVE:

CAPÍTULO I - DISPOSIÇÕES GERAIS

Art. 1º Esta Instrução Normativa estabelece as regras de controle de acesso e os requisitos de segurança para serviços digitais da ATI/TO, aplicando-se a:

- I. servidores efetivos, comissionados e estagiários;
- II. colaboradores terceirizados, consultores e fornecedores;
- III. agentes de outros órgãos que utilizem sistemas geridos pela ATI/TO;
- IV. cidadãos que acessem serviços digitais estaduais.

Art. 2º Para fins desta norma, aplicam-se as definições:

- I. Acesso Privilegiado: acesso que permite ações administrativas, alteração de configurações ou gestão de infraestrutura crítica;
- II. Credencial: conjunto de elementos utilizados para autenticação, incluindo senhas, tokens, certificados e biometria;
- III. MFA - Autenticação Multifator: mecanismo que exige dois ou mais fatores independentes para autenticar o usuário;
- IV. Menor Privilégio: princípio que limita o acesso do usuário ao estritamente necessário para o exercício de suas funções;
- V. Serviço Digital: portal, aplicativo, sistema ou solução tecnológica que permita ao cidadão acessar serviços públicos de forma eletrônica.

Art. 3º O controle de acesso observa os princípios do menor privilégio, da segregação de funções, da rastreabilidade e da responsabilização, sendo toda concessão, alteração ou revogação de acesso obrigatoriamente documentada e rastreável.

CAPÍTULO II - GESTÃO DE CONTAS

Art. 4º Toda conta de usuário deve ser:

I. vinculada a CPF e ao nome completo do titular;

II. associada à unidade, função e tipo de vínculo do usuário;

III. atribuída a um único titular - são vedadas contas compartilhadas, genéricas ou anônimas;

IV. limitada ao perfil de acesso compatível com as atividades desempenhadas.

Parágrafo único. Contas de serviço ou de uso sistêmico podem ser criadas em caráter excepcional, mediante autorização formal da Presidência da ATI/TO e com controles adicionais de monitoramento.

Art. 5º A criação de conta é solicitada pela chefia imediata mediante chamado formal, contendo justificativa da necessidade, perfil de acesso requerido e, quando aplicável, prazo de vigência.

Art. 6º A ativação da conta está condicionada à validação pela ATI/TO, à assinatura do Termo de Responsabilidade e Confidencialidade e à comprovação de ciência das normas de segurança vigentes.

Art. 7º A conta deve ser bloqueada imediatamente em caso de desligamento ou término de contrato, afastamento superior a 30 (trinta) dias, suspeita de comprometimento da credencial ou determinação do ETIR/NIRTI.

Art. 8º A ATI/TO realizará revisão das permissões concedidas, revogando acessos sem necessidade operacional, com duplicidades ou com risco à segurança.

CAPÍTULO III - PERFIS E PRIVILÉGIOS

Art. 9º Os perfis de acesso são:

I. Administrador: acesso privilegiado a sistemas, servidores, bancos de dados e infraestrutura, incluindo criação de usuários e alteração de configurações críticas;

II. Desenvolvedor: acesso a ambientes de desenvolvimento, repositórios e ferramentas técnicas, vedado o acesso direto a dados de produção sem autorização formal;

III. Usuário Padrão: acesso restrito aos sistemas necessários ao desempenho das funções, sem permissões administrativas;

IV. Usuário Externo (cidadão ou fornecedor): acesso limitado ao serviço ou escopo contratual, com permissões mínimas.

Art. 10. Toda elevação de privilégio deve ser temporária, justificada, autorizada formalmente e encerrada assim que a necessidade cessar.

Art. 11. Administradores devem manter conta padrão separada para atividades rotineiras, reservando a conta privilegiada exclusivamente para tarefas que a exijam.

CAPÍTULO IV - ACESSO REMOTO E VPN

Art. 12. O acesso remoto aos sistemas e redes da ATI/TO somente é permitido mediante VPN corporativa homologada, autorização prévia da chefia imediata e dispositivo que atenda aos requisitos mínimos definidos nesta norma.

Art. 13. Os dispositivos utilizados para acesso remoto devem ter sistema operacional atualizado e suportado, solução de antivírus/EDR ativa, firewall habilitado, bloqueio automático de tela e criptografia de disco quando tecnicamente viável.

Art. 14. É proibido no acesso remoto:

- I. utilizar redes públicas sem VPN homologada;
- II. usar dispositivos pessoais sem autorização formal;
- III. compartilhar credenciais de acesso remoto;
- IV. utilizar ferramentas de acesso remoto não homologadas;
- V. manter sessões ativas sem supervisão.

Art. 15. Todo acesso remoto é registrado em log, monitorado e passível de bloqueio automático diante de comportamento anômalo. A ATI/TO poderá suspender acessos imediatamente em caso de risco ou descumprimento desta norma.

CAPÍTULO V - SENHAS E AUTENTICAÇÃO

Art. 16. As senhas devem ter no mínimo 08 (oito) caracteres, combinando letras maiúsculas, minúsculas, números e caracteres especiais, com bloqueio após 5 (cinco) tentativas incorretas, histórico mínimo de 06 (seis) senhas e substituição imediata em caso de comprometimento.

Parágrafo único. A rotação periódica obrigatória sem evidência de comprometimento é desaconselhada, em conformidade com a ISO/IEC 27002:2022. A ATI/TO poderá definir requisitos adicionais para sistemas críticos.

Art. 17. É proibido ao usuário compartilhar senhas ou credenciais, armazená-las em locais inseguros, usar senhas pessoais em sistemas corporativos ou reutilizar a mesma senha em múltiplos sistemas.

CAPÍTULO VI - SERVIÇOS DIGITAIS AO CIDADÃO

Art. 18. Todos os serviços digitais do Governo do Estado do Tocantins que exijam cadastro, autenticação ou identificação do cidadão estão sujeitos a esta Instrução Normativa, incluindo portais de serviços, aplicativos móveis governamentais, sistemas de autosserviço, plataformas de agendamento, emissão de documentos e protocolos digitais.

Art. 19. Os serviços digitais devem implementar obrigatoriamente:

- I. autenticação compatível com o nível de risco do serviço, incluindo MFA para operações de alto impacto;
- II. criptografia de dados em repouso e em trânsito;
- III. segregação dos ambientes de produção, homologação e desenvolvimento;
- IV. proteção contra força bruta, injeção de código, XSS e CSRF;
- V. mecanismos de detecção de acessos anômalos e prevenção a fraudes;
- VI. logs de acesso, operação e transação, retidos conforme a legislação aplicável.

Art. 20. Os serviços digitais devem garantir ao cidadão transparência sobre o uso de seus dados, acesso e possibilidade de correção das informações, canais para exercício dos direitos previstos na LGPD e comunicação clara sobre finalidades e compartilhamentos.

Art. 21. Os órgãos responsáveis por serviços digitais devem:

- I. manter documentação atualizada sobre fluxos de dados e integrações;
- II. realizar testes periódicos de segurança, incluindo testes de intrusão quando aplicável;
- III. comunicar ao ETIR/NIRTI qualquer incidente imediatamente;
- IV. assegurar que terceiros contratados cumpram integralmente esta norma.

Art. 22. AATI/TO poderá definir padrões mínimos de autenticação por tipo de serviço, determinar integração obrigatória com plataformas estaduais de identidade digital e realizar auditorias periódicas de conformidade nos serviços digitais.

CAPÍTULO VII - DISPOSIÇÕES COMPLEMENTARES

Art. 23. No que se refere à proteção de dados pessoais, esta norma é aplicada em conjunto com a LGPD e o Decreto Estadual nº 6.547/2022. O tratamento de dados só pode ocorrer com base legal, para finalidades específicas e pelo menor período necessário, cabendo ao órgão responsável comunicar ao ETIR/NIRTI qualquer incidente de acesso indevido imediatamente.

Art. 24. Incidentes relacionados ao controle de acesso - incluindo acessos não autorizados, comprometimento de credenciais e comportamentos anômalos - devem ser comunicados imediatamente ao ETIR/NIRTI, registrados em sistema próprio e tratados conforme os procedimentos de resposta a incidentes da ATI/TO.

Art. 25. O descumprimento desta norma sujeita o infrator, conforme a gravidade, a: advertência; suspensão de acesso; processo administrativo disciplinar; responsabilização civil e penal; e rescisão contratual, no caso de terceiros. A reincidência ou infração grave deverá ser comunicada ao Ministério Público e à ANPD quando houver envolvimento de dados pessoais.

CAPÍTULO VIII - DISPOSIÇÕES FINAIS

Art. 26. Os casos omissos serão analisados pelo Comitê de Segurança da Informação - CSI da ATI/TO, que poderá emitir orientações complementares ou propor revisão desta norma à Presidência da Agência.

Art. 27. Esta Instrução Normativa será revisada sempre que houver alteração legislativa relevante, mudança tecnológica significativa ou recomendação do ETIR/NIRTI.

Art. 28. Esta Instrução Normativa entra em vigor na data de sua publicação.

ALÍRIO FELIX MARTINS BARROS
Presidente da Agência de Tecnologia da Informação

DETRAN

PORTARIA Nº 290/2026/GABPRES

O PRESIDENTE DO DEPARTAMENTO DE TRÂNSITO DO TOCANTINS - DETRAN/TO de suas atribuições legais, conforme o que consta no §1º, inciso IV, do artigo 42 da Constituição do Estado do Tocantins, constante disposto no Ato nº 3.257 - NM, de 12 de dezembro de 2025, publicado no Diário Oficial do Estado nº 6.960/2025;

CONSIDERANDO que a Administração Pública tem como princípios a legalidade, impessoalidade, moralidade, publicidade e eficiência, de acordo com o disposto no art. 37 da Constituição da República de 1988;

CONSIDERANDO o amparo legal nos termos do art. 74, inciso III, alínea "f" da Lei 14.133/21.

RESOLVE:

Art. 1º INEXIGIR a realização de licitação, com fulcro no amparo legal nos termos do art. 74, inciso III, alínea "f" da Lei 14.133/2021, para a contratação de empresa especializada na realização de curso de capacitação, no valor total de R\$ 24.000,00 (vinte e quatro mil reais), em favor da empresa INSTITUTO NEGÓCIOS PÚBLICOS DO BRASIL ESTUDOS E PESQUISAS NA ADMINISTRAÇÃO PÚBLICA LTDA, CNPJ: 10.498.974/0002-81.

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

Gabinete do Presidente do Detran/TO, em Palmas/TO, aos 31 dias do mês de março de 2026.

HERCY AYRES RODRIGUES FILHO
Presidente do Detran/TO