BOLETIM INTERNO

Publicado em 15/09/2026

TST - Presidência

Assunto: Normativos Internos

ATO TST.GP Nº 519, DE 15 DE SETEMBRO DE 2026

Estabelece parâmetros e diretrizes para a limitação, a suspensão ou o bloqueio do acesso aos sistemas informatizados e aos serviços digitais sob gestão da Secretaria de Tecnologia da Informação e Comunicação do Tribunal Superior do Trabalho, em situações de comportamento inautêntico ou de consumo abusivo de dados.

O PRESIDENTE DO TRIBUNAL SUPERIOR DO TRABALHO, no uso das atribuições legais e regimentais,

considerando o disposto no art. 3º da Resolução CNJ nº 574, de 26 de agosto de 2024, que faculta ao Conselho Nacional de Justiça, ao Conselho da Justiça Federal, ao Conselho Superior da Justiça do Trabalho e aos tribunais a eles vinculados limitar ou bloquear o acesso aos sistemas sob sua coordenação, seja por meio de interface de programação de aplicativos (API) ou não, em caso de comportamento inautêntico ou de consumo abusivo de dados, conforme parâmetros a serem definidos em ato próprio;

considerando o disposto no art. 9º da Portaria CNJ Presidência nº 316, de 20 de setembro de 2024, que, ao regulamentar o acesso a dados judiciais públicos consolidados, define e autoriza a limitação ou o bloqueio do acesso a sistemas ou serviços quando identificado comportamento inautêntico ou consumo abusivo de dados por parte do usuário;

considerando a Portaria STJ/GDG nº 822, de 20 de outubro de 2025, que dispõe sobre parâmetros e diretrizes análogos no âmbito do Superior Tribunal de Justiça, adotada como referência subsidiária;

considerando o Ato GDGSET.GP nº 372, de 27 de junho de 2023 que versa sobre a Política de

Segurança da Informação do Tribunal Superior do Trabalho e a necessidade de assegurar a confidencialidade, a integridade, a autenticidade e a disponibilidade dos sistemas informatizados e serviços digitais institucionais;

considerando o disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e na Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), no que concerne à proteção de dados pessoais e ao tratamento de registros de acesso a aplicações de internet;

considerando os princípios da legalidade, da impessoalidade, da razoabilidade, da proporcionalidade, da motivação, da transparência e da eficiência que regem a Administração Pública;

considerando a necessidade de conciliar a proteção da infraestrutura tecnológica, a continuidade e a estabilidade dos serviços com a preservação do acesso legítimo dos usuários, evitando restrições indevidas a atividades regulares, integrações autorizadas e fluxos críticos de negócio;

considerando o estudo técnico elaborado pelas unidades competentes da Secretaria de Tecnologia da Informação e Comunicação (SETIN), consolidado nos autos do Processo Administrativo TST nº 6005449/2026-00,

RESOLVE

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Este Ato estabelece os parâmetros e as diretrizes para a limitação, o bloqueio ou a suspensão do acesso aos sistemas informatizados e aos serviços digitais sob gestão da Secretaria de Tecnologia da Informação e Comunicação (SETIN) do Tribunal Superior do Trabalho (TST), em situações de comportamento inautêntico ou de consumo abusivo de dados.

Parágrafo único. As medidas de que trata este Ato têm natureza técnica, preventiva ou reativa e não se destinam a restringir o uso legítimo e regular dos sistemas e serviços disponibilizados pelo Tribunal, mas sim a proteger a infraestrutura institucional e a assegurar a continuidade dos serviços.

Art. 2º Para os efeitos deste Ato, consideram-se:

I – autenticidade: garantia de que a origem dos dados ou a identidade de um usuário é genuína;

II – comportamento inautêntico: evento adverso, confirmado ou sob suspeita, que ocorra em desacordo com as normas e diretrizes do Tribunal e indique utilização indevida ou produza comportamentos inesperados dos sistemas informatizados;

III – consumo abusivo de dados: conjunto de ações que, em razão do volume ou da frequência, prejudique ou seja capaz de prejudicar o funcionamento normal dos sistemas informatizados, incluindo requisições excessivas ou automatizadas capazes de sobrecarregar recursos e comprometer o desempenho, a estabilidade, a segurança ou a disponibilidade dos serviços;

IV – credencial de acesso: identificação única do usuário de TIC que concede acesso aos sistemas e ao ambiente de tecnologia da informação e comunicação do Tribunal;

V – dado restrito: dado cujo acesso é limitado e depende de concessão prévia de autorização;

VI – disponibilidade: propriedade que assegura que a informação esteja acessível e utilizável, sob demanda, por usuários de TIC devidamente autorizados;

VII – incidente de segurança da informação: evento adverso, confirmado ou sob suspeita, relacionado à segurança da informação, de sistemas, softwares, dispositivos ou da infraestrutura tecnológica sob a guarda do Tribunal;

VIII – interface de programação de aplicativos (API): conjunto de ferramentas, definições e protocolos que possibilita a comunicação entre plataformas, serviços e sistemas;

IX – sistema informatizado: conjunto organizado de recursos, processos e dados que utiliza tecnologia da informação para coletar, armazenar, processar e disseminar informações, incluindo aplicações, bancos de dados, redes e APIs sob gestão da SETIN;

X – limitação de taxa de requisições (rate limit): mecanismo de controle preventivo que restringe o número de requisições admitidas por origem, credencial, serviço ou canal em determinado intervalo de tempo;

XI – quarentena técnica: medida reativa de restrição temporária, total ou parcial, do acesso de origem, credencial ou usuário associado a comportamento inautêntico ou consumo abusivo;

XII – modo simulado (shadow mode): modalidade de operação em que as regras de controle são avaliadas e registradas sem produzir bloqueio efetivo, destinada à calibragem de limiares e à redução de falsos positivos;

XIII – observabilidade: capacidade de inferir o estado interno dos sistemas a partir da coleta e correlação de telemetria, logs e métricas;

XIV – usuário de TIC: pessoa física ou jurídica que utilize ou interaja com os sistemas informatizados do Tribunal, classificado em:

a) interno: ministro, magistrado convocado, servidor ativo, aposentado, cedido ou licenciado, colaborador e estagiário que possuam identificação na rede de dados do Tribunal;

b) externo: cidadão, advogado, fornecedor ou prestador de serviço;

c) instituição: ente público ou privado, compreendidos os órgãos da administração pública;

d) instituição integrada: usuário de TIC pertencente a instituições que possuam soluções tecnológicas integradas com o Tribunal, inclusive integrações sistêmicas e robôs previamente autorizados.

CAPÍTULO II
DA CARACTERIZAÇÃO DO COMPORTAMENTO INAUTÊNTICO E DO CONSUMO ABUSIVO

Art. 3º Considera-se inautêntico o comportamento do usuário que, por suas características ou circunstâncias, não corresponda ao esperado de um usuário legítimo, incluindo as seguintes hipóteses:

I – utilização de credenciais duplicadas, fictícias ou incompatíveis com a identidade do usuário;

II – utilização não autorizada de rotinas automatizadas que simulem o comportamento humano;

III – execução de múltiplas operações simultâneas;

IV – execução de operações repetitivas em curto espaço de tempo;

V – uso de técnicas ou soluções projetadas para burlar regras e restrições do sistema; ou

VI – uso dos dados para finalidade distinta daquela que justificou o credenciamento.

Art. 4º Considera-se abusivo o consumo de dados realizado em circunstâncias que indiquem extração contínua e em grande escala, apta a comprometer o desempenho, a estabilidade ou a disponibilidade de sistema ou serviço, incluindo, sem prejuízo de outras hipóteses, as seguintes situações:

I – consulta sistemática a processos sem relação direta com o usuário; e

II – extração massiva de petições, documentos ou informações processuais.

Art. 5º A caracterização do comportamento inautêntico e do consumo abusivo observará indicadores técnicos objetivos, tais como:

I – volume de requisições por unidade de tempo incompatível com o uso esperado;

II – número de operações simultâneas por origem ou credencial;

III – repetição intensiva de consultas ou transações em curto intervalo;

IV – padrões de automação incompatíveis com o uso humano ordinário;

V – requisições incompletas ou mal formadas, fora do padrão esperado;

VI – acessos provenientes de endereços IP, provedores de hospedagem ou localizações geográficas atípicas em relação ao histórico do usuário; e

VII – impacto observado no desempenho, na estabilidade ou na disponibilidade dos serviços.

CAPÍTULO III
DOS PRINCÍPIOS E DIRETRIZES

Art. 6º A adoção das medidas previstas neste Ato observará os seguintes princípios e diretrizes:

I – proporcionalidade e gradação: priorização de medidas progressivas e proporcionais à severidade, à recorrência e ao impacto do comportamento identificado;

II – isonomia: aplicação de critérios técnicos uniformes e rastreáveis, de modo a evitar decisões arbitrárias;

III – auditabilidade e rastreabilidade: registro que permita a reconstituição dos eventos e a justificativa objetiva de cada medida aplicada;

IV – preservação da atividade legítima: adoção de parâmetros que evitem afetar indevidamente atividades regulares, integrações autorizadas e fluxos críticos de negócio;

V – transparência: comunicação institucional adequada acerca dos controles adotados e dos meios de restabelecimento de acesso;

VI – revisão periódica: reavaliação dos parâmetros com base em métricas operacionais, incidentes observados e evolução do perfil de consumo dos serviços; e

VII – clareza operacional: definição de critérios suficientemente simples para implementação, monitoramento e comunicação.

Art. 7º Os parâmetros serão definidos de forma segmentada, considerando os diferentes perfis de acesso, notadamente usuários internos, usuários externos, instituições, instituições integradas, integrações sistêmicas, APIs e robôs previamente autorizados, admitida a diferenciação de limiares entre uso humano ordinário, integração autorizada e comportamento suspeito.

CAPÍTULO IV
DA LIMITAÇÃO DE TAXA DE REQUISIÇÕES (RATE LIMIT) – CONTROLE PREVENTIVO

Art. 8º A limitação de taxa de requisições será implementada de forma escalonada, mediante camadas progressivas de resposta, na seguinte ordem de referência:

I – Nível 1 – monitoramento: identificação e registro de padrões atípicos de requisições, endereços IP e geolocalização, sem restrição de acesso;

II – Nível 2 – desafio: exigência de fatores adicionais de validação, tais como desafio CAPTCHA e autenticação multifator, para verificação da origem legítima da requisição;

III – Nível 3 – limitação: redução da taxa admitida ou introdução de atraso controlado na resposta às requisições; e

IV – Nível 4 – bloqueio: recusa temporária das requisições por período determinado.

Art. 9º Os limiares de requisições serão estabelecidos por tipo de serviço, perfil de usuário e canal de acesso e consolidados em Matriz de Parâmetros Técnicos disciplinada em normativo interno da SETIN.

§ 1º A Matriz de Parâmetros Técnicos poderá prever proteções específicas contra fontes de maior potencial de abuso, tais como endereços previamente identificados, acessos oriundos de provedores de hospedagem e requisições provenientes de localidades determinadas.

§ 2º A calibragem inicial dos limites de requisições por origem de acesso para os diversos serviços poderá tomar por referência os controles já implantados no Processo Judicial Eletrônico (PJe) à época da publicação deste Ato.

Art. 10. A resposta às ocorrências será progressiva e proporcional, admitida a combinação dos níveis previstos no art. 8º conforme a severidade, a recorrência e o impacto observado, preservando-se, sempre que possível, o acesso legítimo.

CAPÍTULO V
DA QUARENTENA TÉCNICA – CONTROLE REATIVO

Art. 11. A quarentena técnica será aplicada em situações de abuso confirmado ou de suspeita grave, mediante gatilhos objetivos, tais como tentativas de acesso a dados restritos sem a devida autorização, requisições malformadas não padronizadas ou persistência de padrões de consumo abusivo após a aplicação das medidas preventivas.

Art. 12. A duração da quarentena será temporária e escalonada em razão da reincidência, admitidos, a título exemplificativo, períodos de 15 (quinze) minutos, 1 (uma) hora e 24 (vinte e quatro) horas, conforme detalhado na Matriz de Parâmetros Técnicos.

Art. 13. O acionamento da quarentena observará fluxo de análise, validação e eventual liberação, com registro em trilha de auditoria dos elementos mínimos que fundamentaram a medida.

Art. 14. O usuário submetido a limitação, quarentena ou bloqueio poderá solicitar, independentemente de prévia notificação, o restabelecimento do acesso mediante apresentação de justificativa.

Parágrafo único. Na hipótese do caput, a SETIN decidirá, de forma motivada, sobre o restabelecimento do acesso aos sistemas informatizados do Tribunal.

Art. 15. Em situações de ataque de negação de serviço, exploração indevida de recursos ou risco iminente de indisponibilidade, a equipe técnica fica autorizada a aplicar medidas emergenciais de contingência, incluindo a restrição temporária de tráfego por origem ou localização geográfica, devendo a medida ser posteriormente documentada e reportada.

CAPÍTULO VI
DO MONITORAMENTO, DA OBSERVABILIDADE E DA AUDITORIA

Art. 16. Para assegurar o nexo causal entre a conduta e o impacto, a infraestrutura deverá coletar, no mínimo:

I – telemetria de rede, com o volume de requisições simultâneas e os picos de carga por serviço;

II – registros (logs) de erros das classes 4xx e 5xx associados a acessos automatizados; e

III – métricas de desempenho, notadamente disponibilidade (uptime) e latência, de modo a evitar falsos positivos que afetem usuários legítimos.

Art. 17. Os eventos de limitação, quarentena e bloqueio serão registrados com os elementos mínimos necessários à sua reconstituição, observados os prazos de retenção definidos pela

Política de Segurança da Informação e pela legislação aplicável.

Art. 18. A SETIN promoverá a correlação dos eventos coletados, de modo a demonstrar o nexo entre a conduta identificada e o impacto operacional, subsidiando as decisões técnicas.

CAPÍTULO VII
DA GOVERNANÇA, DAS COMPETÊNCIAS E DA REVISÃO

Art. 19. A implementação, o monitoramento e a revisão das medidas previstas neste Ato serão acompanhados pela Coordenadoria de Governança e Evolução Digital (CGDIGITAL), com a participação das demais unidades da SETIN, no âmbito de suas competências, notadamente:

I – compete à Coordenadoria de Infraestrutura Tecnológica (CITEC) a análise técnica de capacidade e do funcionamento dos bens e serviços de infraestrutura, redes e gateways de API;

II – compete à Coordenadoria de Desenvolvimento de Sistemas (CDS) o tratamento dos sistemas administrativos sob sua responsabilidade, especialmente os de acesso público ou voltados à transparência institucional;

III – compete à Coordenadoria de Segurança Cibernética (CSEC) a análise sob a ótica da segurança da informação e a coordenação da resposta a incidentes;

IV – compete à Coordenadoria do PJe (CPJe) a manutenção e a evolução dos controles no âmbito do Processo Judicial Eletrônico; e

V – compete à Coordenadoria de Suporte (CSUP) o apoio às atividades de operação, monitoramento e atendimento correlatas.

Art. 20. Previamente à entrada em produção de novos limiares ou regras, a SETIN adotará, sempre que viável, fase de operação em modo simulado (shadow mode), destinada à calibragem dos parâmetros e à mitigação de impactos sobre integrações autorizadas e usuários legítimos.

Art. 21. A Matriz de Parâmetros Técnicos será revisada periodicamente, ao menos uma vez por ano, ou sempre que houver alteração relevante do perfil de consumo dos serviços, dos incidentes observados ou dos requisitos normativos.

Art. 22. O Tribunal dará publicidade, na medida adequada e sem comprometer a eficácia dos controles, às diretrizes de uso aceitável e aos meios de restabelecimento de acesso.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS

Art. 23. Em caso de bloqueio ou de suspensão de acesso decorrente de comportamento inautêntico ou de consumo abusivo, a SETIN comunicará o fato à Administração Superior, para avaliação da conveniência de comunicação, conforme o caso, à autoridade competente, com vistas à identificação e à responsabilização dos responsáveis pela conduta.

Art. 24. O usuário que tiver seu acesso limitado, suspenso ou bloqueado poderá solicitar orientações, comunicar eventual indisponibilidade ou requerer apoio técnico à SETIN, por meio do endereço eletrônico suporte@tst.jus.br ou da Central de Atendimento, sem prejuízo do disposto no art. 14 deste Ato.

Art. 25. Este Ato será objeto de revisão no prazo de 12 (doze) meses, contado da data de sua publicação.

Art. 26. Os casos omissos serão dirimidos pelo Presidente do Tribunal Superior do Trabalho.

Art. 27. Este Ato entra em vigor na data de sua publicação.

VIEIRA DE MELLO FILHO

Ministro Presidente