Caderno Administrativo
Conselho Superior da Justiça do Trabalho

DIÁRIO ELETRÔNICO DA JUSTIÇA DO TRABALHO

PODER JUDICIÁRIO

REPÚBLICA FEDERATIVA DO BRASIL

Nº4475/2026 **Data da disponibilização: Quarta-feira, 20 de Maio de 2026.**

Setor de Administração Federal Sul (SAFS) Quadra 8 - Lote 1,
Zona Cívico-Administrativa, Brasília/DF
CEP: 70070943

Telefone(s) : (61) 3043-7961
(61) 3043-3804

Conselho Superior da Justiça do Trabalho

Ato

Ato da Presidência CSJT

ATO CSJT.GP.SG.SETIC N.º 53, DE 19 DE MAIO DE 2026.

Institui o conjunto de Soluções Essenciais de Tecnologia da Informação e Comunicação (TIC) na Justiça do Trabalho de primeiro e segundo graus.

O **PRESIDENTE DO CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO**, no uso de suas atribuições regimentais,

considerando o disposto na Resolução CSJT n.º 364, de 29 de setembro de 2023, que dispõe sobre a Política de Governança e Gestão das Contratações da Justiça do Trabalho de primeiro e segundo graus;

considerando o disposto na Resolução CSJT n.º 425, de 28 de outubro de 2025, que institui a Política de Governança de Tecnologia da Informação e Comunicação da Justiça do Trabalho de primeiro e segundo graus (PGTIC-JT);

considerando a necessidade de assegurar a continuidade dos serviços institucionais suportados por soluções de Tecnologia da Informação e Comunicação;

considerando a necessidade de padronizar o planejamento, a priorização e a execução orçamentária das contratações de TIC;

considerando a necessidade de garantir rastreabilidade, transparência e gestão de riscos no processo orçamentário; e

considerando o teor do Processo Administrativo SEI n.º 6010209/2026-00,

RESOLVE

Art. 1º Fica instituído, nos termos do Anexo Único deste Ato, o Conjunto de Soluções Essenciais de Tecnologia da Informação e Comunicação (TIC) no âmbito da Justiça do Trabalho de primeiro e segundo graus, em cumprimento ao art. 30, § 3º da Resolução CSJT n.º 425, de 28 de outubro de 2025.

Parágrafo único. Nos termos do art. 2º, inciso XXI, da Resolução CSJT n.º 425, de 28 de outubro de 2025, consideram-se Soluções Essenciais aquelas cuja interrupção impacta o funcionamento normal do órgão, impedindo o cumprimento de suas obrigações institucionais.

Art. 2º Todas as soluções constantes do Anexo Único são classificadas como essenciais, devendo ser priorizadas, observando as diretrizes da Resolução CSJT n.º 364, de 29 de setembro de 2023, bem como o planejamento e a execução orçamentária.

Parágrafo único. Na eventual impossibilidade de atendimento integral dessas soluções no período, orienta-se que a priorização observe o campo "prioridade", de modo a subsidiar a seleção daquelas que constarão no planejamento de contratação, cabendo, neste caso, o mapeamento dos riscos decorrentes do não atendimento das demais soluções.

Art. 3º Revoga-se o Ato CSJT.GP.SG.SETIC.CGTIC n.º 132, de 14 de setembro de 2022.

Art. 4º Este Ato entra em vigor na data de sua publicação.

VIEIRA DE MELLO FILHO
Ministro Presidente do Conselho Superior da Justiça do Trabalho

ANEXO ÚNICO

LISTA DE SOLUÇÕES ESSENCIAIS ART. 1º DO ATO CSJT.GP.SG.SETIC N.º 53, DE 19 DE MAIO DE 2026

ID	MARCADOR SIGEO	IDENTIFICAÇÃO DA SOLUÇÃO	PRIORIDADE	ESCOPO	ORIENTAÇÕES GERAIS	IMPACTO PARA O TRIBUNAL
1	ANÁLISE DE DADOS, APRENDIZADO DE MÁQUINA E INTELIGÊNCIA ARTIFICIAL	Business Intelligence (BI) - Licenciamento *desktop*	MÉDIA	Licenciamento de ferramenta de BI em ambiente *desktop* para desenvolvimento, edição e publicação de painéis e relatórios, com integração à plataforma corporativa institucional.	Realizar o licenciamento de ferramentas *desktop* de BI em conformidade com processos de aquisição compartilhada nacional, assegurando padronização, compatibilidade com a solução centralizada e otimização de custos.	A ausência de uma ferramenta de BI pode gerar os seguintes impactos: - Restrição de publicação e compartilhamento, quebrando o fluxo de disseminação da informação. - Perda de integração com a plataforma institucional, trazendo fragmentação da informação e retrabalho. - Redução da capacidade analítica, resultando em análises menos robustas e menor apoio à tomada de decisão. - Impacto na padronização e governança, dificuldade de auditoria e controle.

2	COMPUTAÇÃO EM NUVEM	Computação em Nuvem	ALTA	Fornecimento de serviços de infraestrutura (IaaS), plataforma (PaaS) ou serviço (Saas) sob demanda para sustentação de produtos digitais nacionais.	Dentre as soluções de grau de urgência ALTA, esta tem maior criticidade. Planejar, contratar e gerenciar serviços de computação em nuvem (IaaS, PaaS e SaaS) de forma alinhada às diretrizes do CSJT, com monitoramento contínuo de consumo, desempenho, custos e disponibilidade, garantindo sustentação adequada dos produtos digitais.	A ausência de créditos de nuvem e a gestão inadequada pode resultar em indisponibilidade de produtos digitais críticos, interrupção de serviços institucionais e impactos diretos na continuidade das atividades judiciais e administrativas.
3	COMUNICAÇÃO DE DADOS	*Links* e Conectividade	ALTA	Prestação de serviços de conectividade de dados, incluindo *links* dedicados, acesso à internet de alta disponibilidade, interconexão entre unidades e gestão de tráfego de rede.	Dentre as soluções de grau de urgência ALTA, esta tem maior criticidade. Implementar gestão contínua dos serviços de conectividade, com monitoramento de desempenho, planejamento de capacidade e adoção de mecanismos de redundância, assegurando alta disponibilidade e qualidade da comunicação de dados.	A indisponibilidade ou degradação da conectividade compromete o acesso aos produtos digitais institucionais, podendo paralisar atividades essenciais e afetar diretamente a prestação jurisdicional.
4	COMUNICAÇÃO DE DADOS	Rede Local (LAN)	ALTA	Aquisição, suporte e manutenção de equipamentos de rede local (*switches*, roteadores, *access points* e controladoras Wi-Fi), incluindo configuração, gerenciamento e garantia de funcionamento.	Gerenciar o ciclo de vida dos ativos de rede local, garantindo atualização tecnológica, suporte e manutenção contínua, bem como adequação da capacidade à demanda institucional.	Falhas na rede local impedem o acesso a sistemas e produtos digitais institucionais, comprometendo a produtividade e a continuidade das atividades do Tribunal.

5	COMUNICAÇÃO DE DADOS	Rede de Armazenamento (SAN)	ALTA	Soluções de rede de alta velocidade para interconexão entre servidores e sistemas de armazenamento, incluindo *switches* SAN, cabeamento especializado e suporte técnico.	Dentre as soluções de grau de urgência ALTA, esta tem maior criticidade. Monitorar e planejar a capacidade, desempenho e obsolescência da infraestrutura de rede de armazenamento, garantindo suporte técnico adequado e compatibilidade com as demandas de processamento e acesso a dados.	Problemas na rede SAN podem causar lentidão ou indisponibilidade no acesso a dados críticos, impactando diretamente sistemas judiciais e administrativos.
6	COMUNICAÇÃO DE DADOS	Videoconferência	ALTA	Fornecimento de plataformas, licenças e infraestrutura para realização de videoconferências institucionais, incluindo audiências telepresenciais e sessões de julgamento, com suporte técnico associado.	Adotar e manter soluções de videoconferência alinhadas aos padrões nacionais definidos, garantindo interoperabilidade, estabilidade, segurança e suporte às atividades institucionais, especialmente audiências e sessões de julgamento.	A indisponibilidade dessas soluções pode resultar na suspensão de audiências e sessões, causando atrasos na prestação jurisdicional e prejuízos processuais.

7	INFRAESTRUTURA DE TIC	Virtualização	ALTA	Licenciamento e suporte de *softwares* de virtualização (*hypervisors*) para criação, gestão e operação de ambientes virtuais em infraestrutura local.	Avaliar a adoção e manutenção de soluções de virtualização de servidores em ambientes locais (*on-premises*), considerando o alinhamento com a estratégia institucional de computação em nuvem e evitando sobreposição de camadas tecnológicas, que no caso da nuvem, passa a ser do provedor. Nos casos em que a virtualização local se mostrar necessária, o Tribunal deve garantir licenciamento adequado, suporte técnico, atualização contínua e compatibilidade com a infraestrutura existente, assegurando eficiência operacional, segurança e otimização do uso de recursos computacionais.	Para o tribunal que utiliza tais plataformas de virtualização, a ausência de licenciamento e suporte adequado compromete diretamente a continuidade, a segurança e a eficiência dos serviços de TIC em ambientes *on-premises*. Sem suporte oficial e atualizações regulares, aumentam os riscos de indisponibilidade prolongada, falhas críticas e exposição a vulnerabilidades conhecidas, além de dificultar a recuperação de ambientes e a adoção de boas práticas de segurança. A ausência de licenciamento também favorece a obsolescência tecnológica, gerando incompatibilidades com novas soluções e limitando a evolução da infraestrutura.

8	INFRAESTRUTURA DE TIC	Infraestrutura de *Data Center*	ALTA	Manutenção, operação e modernização da infraestrutura física de *data center*, incluindo salas-cofre, sistemas de climatização, fornecimento e condicionamento de energia (*nobreaks*, bancos de baterias e geradores), sistemas de detecção e combate a incêndio, controle de acesso físico e monitoramento ambiental, bem como serviços associados de suporte técnico e manutenção preventiva e corretiva.	Dentre as soluções de grau de urgência ALTA, esta tem maior criticidade. Garantir a adequada gestão da infraestrutura física de data center, incluindo salas-cofre, sistemas de climatização, fornecimento de energia (*nobreaks* e geradores) e mecanismos de segurança física. O Tribunal deve realizar monitoramento contínuo do ambiente, manutenção preventiva e corretiva, bem como o gerenciamento do ciclo de vida e da obsolescência dos equipamentos, assegurando conformidade com normas técnicas aplicáveis e requisitos de continuidade de negócio.	Falhas na infraestrutura física do *data center* podem ocasionar indisponibilidade total ou parcial dos sistemas institucionais, com impactos severos na continuidade das atividades judiciais e administrativas. Eventos como interrupções de energia, falhas de climatização ou incidentes físicos (incêndio, alagamento, entre outros) podem comprometer a integridade dos ativos tecnológicos, causar perda de dados e gerar prejuízos operacionais e institucionais significativos.

9	INFRAESTRUTURA DE TIC	Monitoramento de TIC	MÉDIA	Implantação, configuração e sustentação de soluções de monitoramento e observabilidade do ambiente de TIC, incluindo coleta de métricas, *logs* e *traces*, acompanhamento de desempenho, disponibilidade e capacidade de ativos e serviços (servidores, redes, aplicações e banco de dados), com utilização de ferramentas especializadas (ex.: Zabbix, Grafana ou equivalentes), integração entre plataformas e geração de alertas, painéis e relatórios gerenciais.	Adotar solução de monitoramento alinhada às diretrizes institucionais e, quando aplicável, aos padrões definidos pelo CSJT para produtos digitais nacionais, garantindo cobertura abrangente do ambiente tecnológico. O Tribunal deve assegurar a correta parametrização de alertas, definição de indicadores (KPIs), integração com processos de gestão de incidentes e manutenção contínua da solução, visando suporte à operação e à tomada de decisão.	A ausência de soluções adequadas de monitoramento e observabilidade, como Zabbix e Grafana, reduz a visibilidade sobre o ambiente de TIC, dificultando a identificação rápida de falhas, degradações de desempenho e problemas de capacidade. Sem coleta estruturada de métricas, *logs* e *traces*, bem como alertas e indicadores (KPIs) bem definidos, a atuação torna-se reativa, aumentando o tempo de resposta a incidentes e o risco de indisponibilidade de serviços. Além disso, a falta de integração com processos institucionais e a ausência de padronização comprometem a governança, elevam a complexidade operacional e prejudicam a tomada de decisão, podendo resultar em ineficiência e aumento de custos.
10	INFRAESTRUTURA DE TIC	Servidores de Aplicação	MÉDIA	Licenciamento, suporte e manutenção de servidores de aplicação e *middlewares* responsáveis pelo processamento das regras de negócio dos sistemas institucionais.	Adotar soluções de servidores de aplicação (*middlewares*) devidamente homologadas, licenciadas e alinhadas às diretrizes institucionais e às soluções nacionais estabelecidas pelo CSJT. Deve-se garantir suporte técnico contínuo, atualização tecnológica e compatibilidade com os sistemas corporativos, assegurando estabilidade, segurança e desempenho das aplicações.	A ausência de licenciamento, suporte e manutenção de servidores de aplicação e *middlewares*, compromete diretamente a estabilidade, a segurança e o desempenho dos sistemas institucionais. Sem suporte técnico e atualizações contínuas, aumentam os riscos de falhas, vulnerabilidades e incompatibilidades com outras soluções corporativas, dificultando a evolução tecnológica e a integração entre sistemas. A ausência de manutenção adequada pode gerar degradação de performance e indisponibilidade de serviços críticos, impactando a operação institucional.

11	INFRAESTRUTURA DE TIC	*Storage* (Armazenamento Local)	ALTA	Aquisição e manutenção de soluções de armazenamento local de dados, incluindo *storages*, discos, controladoras e mecanismos de redundância e alta disponibilidade.	Dentre as soluções de grau de urgência ALTA, esta tem maior criticidade. Planejar e gerenciar a infraestrutura de armazenamento local, considerando capacidade, desempenho, redundância e suporte técnico, com monitoramento contínuo do ciclo de vida e da obsolescência dos equipamentos.	Falhas ou insuficiência de armazenamento podem resultar em indisponibilidade de sistemas, perda de dados e comprometimento da continuidade das operações institucionais.
12	INFRAESTRUTURA DE TIC	*Backup* e Recuperação	ALTA	Implementação de soluções de *backup* e recuperação de dados, incluindo *softwares*, mídias de armazenamento (fitas, discos), bibliotecas automatizadas e serviços de restauração.	Implementar política abrangente de *backup* e recuperação de dados, contemplando rotinas automatizadas, testes periódicos de restauração e armazenamento seguro das cópias, observando, para ambientes em nuvem, as diretrizes estabelecidas pelo CSJT.	A inexistência ou falha nos mecanismos de *backup* impede a recuperação de dados e sistemas em situações de incidentes, podendo ocasionar perda irreversível de informações e paralisação prolongada das atividades.
13	INFRAESTRUTURA DE TIC	Servidores Físicos	ALTA	Aquisição, suporte e manutenção de servidores físicos destinados ao processamento de dados em ambiente local, incluindo garantia e serviços associados.	Dentre as soluções de grau de urgência ALTA, esta tem maior criticidade. Gerenciar o ciclo de vida dos servidores físicos, assegurando capacidade adequada, suporte técnico, atualização tecnológica e alinhamento com a estratégia de uso de ambientes locais e em nuvem.	A indisponibilidade ou falha desses equipamentos compromete o processamento de dados e a execução de sistemas, afetando diretamente a continuidade das atividades institucionais.

14	INFRAESTRUTURA DE TIC	Banco de Dados (SGBD)	ALTA	Licenciamento, suporte e manutenção de sistemas gerenciadores de banco de dados (SGBD) em ambiente local, incluindo instalação, configuração, atualização e suporte técnico especializado.	Garantir o licenciamento regular, suporte técnico especializado e atualização contínua dos sistemas gerenciadores de banco de dados, observando, para ambientes em nuvem, as diretrizes do CSJT, bem como práticas de segurança, desempenho e alta disponibilidade.	A ausência de suporte ou uso inadequado pode gerar indisponibilidade de sistemas, perda de dados, riscos jurídicos e dificuldades na recuperação em situações de falha ou desastre.
15	MATERIAIS E EQUIPAMENTOS DE TIC	*Desktops*	BAIXA	Aquisição de estações de trabalho do tipo *desktop*, incluindo periféricos, licenciamento de sistema operacional, garantia e suporte técnico.	Planejar a aquisição e renovação de *desktops* com base no ciclo de vida dos equipamentos, disponibilidade de suporte, atualizações de segurança e necessidades institucionais, considerando expansão ou reestruturação organizacional.	Equipamentos obsoletos ou sem suporte podem comprometer a produtividade, causar paralisação de atividades e dificultar a reposição, impactando a continuidade dos serviços.
16	MATERIAIS E EQUIPAMENTOS DE TIC	*Notebooks*	MÉDIA	Aquisição de *notebooks* destinados a atividades itinerantes ou externas, incluindo suporte técnico, garantia e configuração para uso institucional.	Prever, no planejamento anual, a aquisição e manutenção de *notebooks* destinados a atividades itinerantes ou externas, garantindo suporte técnico, segurança e atualização tecnológica adequada ao uso institucional.	A indisponibilidade ou inadequação desses equipamentos pode comprometer atividades externas e itinerantes, impactando a prestação jurisdicional e a execução de ações institucionais.

17	MATERIAIS E EQUIPAMENTOS DE TIC	*Notebooks*	BAIXA	Aquisição de *notebooks* para uso institucional geral, incluindo manutenção, suporte técnico e adequação às necessidades operacionais do Tribunal.	Avaliar a necessidade de aquisição e renovação de *notebooks* com base na disponibilidade orçamentária, no ciclo de vida dos equipamentos, na existência de suporte e na demanda institucional, garantindo alinhamento com a estratégia de uso de recursos de TIC.	Protelar a substituição desse tipo de equipamento pode impactar negativamente nas atividades que são desenvolvidas por meio dele, afetando a produtividade e continuidade das atividades.
18	SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE	Proteção de *Endpoint*	ALTA	Proteção contra *malwares* e ameaças em estações de trabalho e servidores, com suporte e gestão centralizada.	Implementar solução corporativa de proteção de *endpoints* (Endpoint Security), abrangendo estações de trabalho e servidores, com funcionalidades de antivírus, *antimalware*, detecção e resposta a incidentes (EDR/XDR), gestão centralizada e atualização contínua de assinaturas e políticas de segurança. A solução deve possibilitar monitoramento em tempo real, aplicação de políticas padronizadas e geração de relatórios para fins de auditoria e conformidade.	A ausência ou inadequação de proteção de *endpoints* expõe o ambiente institucional a infecções por *malware*, *ransomware* e outras ameaças cibernéticas, podendo resultar em indisponibilidade de sistemas, comprometimento ou perda de dados sensíveis e interrupção das atividades judiciais e administrativas, além de riscos à imagem institucional.

19	SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE	Proteção de Perímetro	ALTA	Implementação de soluções de segurança de rede, incluindo *firewall*, VPN, WAF e sistemas de detecção e prevenção de intrusões (IDS/IPS).	Dentre as soluções de grau de urgência ALTA, esta tem maior criticidade. Implementar e manter soluções de proteção de perímetro, incluindo *firewall*, VPN, WAF e mecanismos de detecção e prevenção de intrusões (IDS/IPS), garantindo configuração adequada, atualização contínua e monitoramento permanente. Para ambientes em nuvem, devem ser observadas as diretrizes e padrões definidos pelo CSJT (Centro de Excelência em Nuvem), assegurando conformidade, integração e proteção das fronteiras da rede institucional.	A ausência ou inadequação dos mecanismos de proteção de perímetro expõe o ambiente institucional a acessos não autorizados, ataques cibernéticos e exploração de vulnerabilidades, podendo resultar em indisponibilidade de sistemas, vazamento de dados sensíveis e comprometimento da continuidade das atividades judiciais e administrativas.

20	SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE	Gestão de Acessos (IAM)	ALTA	Implantação de solução de gestão de identidades e acessos, incluindo autenticação, controle de permissões e gerenciamento de credenciais.	Dentre as soluções de grau de urgência ALTA, esta tem maior criticidade. Adotar solução de gestão de identidades e acessos (IAM) que permita controle centralizado, autenticação forte, gestão de credenciais e definição de perfis de acesso com base no princípio do menor privilégio. Para ambientes em nuvem, deve-se observar os padrões estabelecidos pelo CSJT, garantindo integração com os sistemas institucionais e rastreabilidade das ações dos usuários.	A inexistência ou fragilidade na gestão de acessos pode resultar em concessão indevida de privilégios, acessos não autorizados e dificuldade de auditoria, elevando o risco de incidentes de segurança, vazamento de informações sensíveis e responsabilização institucional.
21	SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE	Gestão de Eventos	ALTA	Coleta e análise de *logs* para detecção antecipada de ameaças cibernéticas e incidentes de segurança.	Implementar solução para coleta, correlação e análise de eventos de segurança (*logs*), possibilitando monitoramento contínuo, detecção precoce de incidentes e suporte a investigações. A solução deve garantir retenção adequada dos registros, integridade das informações e capacidade de auditoria, preferencialmente integrada a ferramentas de SIEM.	A ausência de gestão adequada de eventos impede a identificação tempestiva de incidentes de segurança, dificulta a análise forense e inviabiliza a rastreabilidade de ações no ambiente computacional, aumentando significativamente o risco de danos prolongados e não detectados.

22	SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE	Gestão de Vulnerabilidades	ALTA	Implementação de soluções para identificação, análise e correção de vulnerabilidades, incluindo varreduras automatizadas e testes de intrusão.	Uma vez detectada, o Tribunal deverá atuar para a correção da vulnerabilidade, mantendo informações suficientes para verificação futura	O Tribunal ficará vulnerável, deixando-o exposto a ataques que colocam em risco dados importantes para a continuidade do negócio, bem como a execução de suas atividades
23	SOFTWARE E APLICATIVOS	Plataforma de Colaboração	ALTA	Fornecimento de plataforma integrada de colaboração, incluindo e-mail, comunicação instantânea, armazenamento e edição de documentos e ferramentas de produtividade.	Dentre as soluções de grau de urgência ALTA, esta tem maior criticidade. Adotar plataforma de colaboração institucional padronizada, preferencialmente e alinhada à solução definida em âmbito nacional, contemplando funcionalidades de correio eletrônico, comunicação instantânea, videoconferência, armazenamento e edição colaborativa de documentos. Em processos de contratação ou renovação, o Tribunal deve observar a aderência às diretrizes do CSJT, assegurando interoperabilidade, segurança da informação e integração entre unidades.	A utilização de soluções não padronizadas pode ocasionar fragmentação das informações institucionais, dificultando a comunicação e a colaboração entre as unidades organizacionais. Adicionalmente, pode gerar ineficiência operacional, aumento de custos, riscos à segurança da informação e prejuízos à governança e à gestão do conhecimento no âmbito do Tribunal.

24	SUPORTE E ATENDIMENTO A USUÁRIO DE TIC	Serviço de Atendimento ao Usuário (Service Desk)	MÉDIA	Implantação e operação de solução de atendimento ao usuário de TIC (Service Desk), incluindo registro, categorização, acompanhamento e resolução de demandas.	Implementar e manter solução de Serviço de Atendimento alinhada às diretrizes estabelecidas na Resolução CSJT nº 397/2024, especialmente quanto à obrigatoriedade de registro, categorização, priorização e acompanhamento das demandas de TIC. A solução deve estar integrada ao Planejamento de Contratações de Soluções de TIC (PCSTIC) do Tribunal, possibilitando gestão centralizada, mensuração de níveis de serviço (SLAs), rastreabilidade dos atendimentos e geração de indicadores para apoio à governança e melhoria contínua dos serviços.	A ausência ou inadequação de solução de Service Desk pode resultar em desconformidade normativa, fragilidade na gestão das demandas de TIC e aumento da dependência de processos informais ou manuais. Isso tende a provocar maior tempo de resposta e resolução de incidentes, impactando diretamente a continuidade das atividades das unidades organizacionais, além de reduzir a transparência, a eficiência operacional e o nível de satisfação dos usuários internos.

25	SUPORTE E ATENDIMENTO A USUÁRIO DE TIC	Suporte a infraestrutura de produtos diginais nacionais	MÉDIA	Prestação de serviços especializados de suporte técnico à infraestrutura de TIC que sustenta os produtos digitais nacionais, incluindo atendimento a incidentes, requisições de serviço, *troubleshooting*, monitoramento assistido, atuação preventiva e corretiva em ambientes computacionais	Estruturar e manter serviços de suporte técnico à infraestrutura de TIC alinhados às diretrizes dos produtos digitais nacionais e aos normativos do CSJT, garantindo integração com a central de serviços (Service Desk), definição de níveis de serviço (SLAs), fluxos de atendimento e responsabilidades claras entre as equipes envolvidas. O suporte deve contemplar atuação preventiva e corretiva, registro e rastreabilidade das demandas, bem como geração de indicadores para monitoramento da qualidade e melhoria contínua dos serviços.	A ausência ou inadequação do suporte à infraestrutura compromete a sustentação dos produtos digitais nacionais, aumentando o tempo de resolução de incidentes e o risco de indisponibilidade dos sistemas institucionais. Isso pode impactar diretamente a continuidade das atividades judiciais e administrativas, reduzir a eficiência operacional e comprometer o cumprimento de níveis de serviço, além de gerar riscos à governança e à qualidade dos serviços prestados.

Legenda	
Marcador SIGEO	Campo do SIGEO utilizado para identificar o tipo de contratação e a natureza da solução. Utiliza-se como referência o Anexo II daInstrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022
Identificação da solução	Rótulo para identificar a solução tecnológica que está sendo planejada
Prioridade	Todas as soluções listadas são classificadas como essenciais e, portanto, devem ser priorizadas pelo Tribunal. Contudo, na eventual impossibilidade de atendimento integral dessas soluções no período, orienta-se que a priorização observe o campo 'PRIORIDADE', de modo a subsidiar a seleção daquelas que constarão no planejamento de contratação, cabendo, neste caso, o mapeamento dos riscos decorrentes do não atendimento das demais soluções.
Escopo	Descrição das ferramentas e serviços que podem ser classificadas dentro da solução tecnológica que está sendo planejada
Orientações Gerais	Diretrizes que devem ser avaliadas pelo Tribunal em seu planejamento
Impacto para o Tribunal	Um breve panorama das possíveis consequências assumidas pelo Tribunal em caso de não prover o orçamento adequado da solução tecnológica

ATO CSJT.GP.SG.SETIC N.º 54, DE 19 DE MAIO DE 2026.