



TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA

GABINETE DA CORREGEDORIA GERAL

PROCESSO: SEI N. 001808/2026

ASSUNTO: DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO APLICÁVEIS AO TELETRABALHO TEMPORÁRIO DECORRENTE DE OBRAS NO EDIFÍCIO-SEDE

DECISÃO N. 9/2026-CG

ADMINISTRATIVO. ATO DE ORIENTAÇÃO INSTITUCIONAL. TRABALHO REMOTO TEMPORÁRIO. SEGURANÇA DA INFORMAÇÃO. OBSERVÂNCIA DAS POLÍTICAS CORPORATIVAS DE SEGURANÇA DA INFORMAÇÃO. PREVENÇÃO DE CONFLITO DE INTERESSES. RESPONSABILIDADE FUNCIONAL DOS AGENTES PÚBLICOS. EXPEDIÇÃO DE DIRETRIZES.

I – Caso em exame

1. Decisão destinada a estabelecer orientações institucionais aos agentes públicos deste Tribunal em razão da adoção temporária do regime de trabalho remoto decorrente de intervenções estruturais no edifício-sede, com foco na preservação da segurança da informação, na proteção dos ativos informacionais e na continuidade regular das atividades institucionais.

II – Questão em discussão

2. A questão em discussão consiste em reforçar os parâmetros institucionais para o exercício do trabalho remoto, especialmente quanto: (i) à observância das diretrizes de segurança da informação estabelecidas pela Secretaria Estratégica de Tecnologia da Informação e Comunicação; (ii) à utilização de ambientes adequados à execução das atividades funcionais; e (iii) à prevenção de situações que possam comprometer a confidencialidade das informações institucionais, a independência funcional ou gerar potenciais conflitos de interesses.

III – Razões de decidir

3. O regime de teletrabalho mantém íntegros os deveres funcionais inerentes ao exercício do cargo ou função pública, inclusive quanto à proteção dos dados institucionais, à segurança dos sistemas corporativos e à observância das políticas corporativas de governança e integridade.

4. A ampliação do acesso remoto aos sistemas institucionais demanda reforço das medidas de segurança da informação, especialmente quanto ao uso de redes seguras, à utilização exclusiva de equipamentos para fins laborais e à adoção de cautelas destinadas a impedir o acesso indevido de terceiros às informações institucionais.

5. O exercício das atividades em ambientes inadequados ou vinculados a atividades privadas potencialmente relacionadas ao campo de atuação do Tribunal pode comprometer a confidencialidade das informações, a independência funcional do agente público e a percepção de integridade institucional, impondo-se a adoção de diretrizes preventivas para mitigação desses riscos.

6. O descumprimento das diretrizes de segurança da informação e das cautelas funcionais estabelecidas poderá ensejar a apuração de responsabilidade administrativa individual, nos termos das normas institucionais aplicáveis.

IV – Dispositivo

7. Expedição de orientações institucionais aos agentes públicos deste Tribunal para observância obrigatória das diretrizes de segurança da informação e das cautelas funcionais aplicáveis ao

1. Considerando a necessidade de adoção temporária do regime de trabalho remoto por parte de servidores e colaboradores deste Tribunal, em razão das intervenções estruturais em curso no edifício-sede, reputa-se necessário registrar orientações institucionais destinadas a assegurar a regular continuidade das atividades e, especialmente, a preservação da segurança da informação no âmbito desta Corte de Contas.
2. Nos termos da regulamentação interna, o teletrabalho constitui modalidade de jornada diferenciada em que o servidor executa suas atribuições funcionais fora das dependências do Tribunal, mediante o uso de equipamentos e tecnologias que permitam a plena execução das atividades institucionais, permanecendo integralmente submetido às metas, responsabilidades funcionais e deveres institucionais inerentes ao exercício do cargo ou função pública (Resolução n. 305/2019).
3. A adoção dessa modalidade, entretanto, impõe redobrada atenção às medidas de proteção dos ativos informacionais do Tribunal, especialmente porque o ambiente remoto amplia potenciais vetores de risco relacionados ao acesso indevido a sistemas corporativos, à exposição de dados institucionais e à integridade das informações sob custódia desta Corte.
4. Nesse contexto, cumpre enfatizar que todos os agentes públicos em regime de trabalho remoto deverão observar rigorosamente as diretrizes de segurança da informação estabelecidas pela Secretaria Estratégica de Tecnologia da Informação e Comunicação – SETIC, bem como as normas e princípios previstos na Política Corporativa de Segurança da Informação e no Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados, instituídos pela Resolução n. 377/2022, que estabelecem o dever institucional de proteção dos dados, sistemas e ativos informacionais do Tribunal.
5. Dessa forma, constituem obrigações funcionais indeclináveis dos agentes públicos que atuarem em regime remoto, entre outras medidas correlatas:
 - (i) realizar o acesso aos sistemas institucionais exclusivamente por meio das soluções tecnológicas autorizadas pela SETIC, observando os mecanismos de autenticação e proteção disponibilizados;
 - (ii) utilizar apenas redes seguras e protegidas por senha, sendo vedado o acesso por meio de redes públicas ou ambientes que comprometam a segurança da informação;
 - (iii) empregar os equipamentos utilizados para acesso aos sistemas institucionais exclusivamente para fins laborais, vedado seu compartilhamento com terceiros;
 - (iv) manter atualizados os sistemas e aplicações, bem como preservar os mecanismos de segurança instalados nos equipamentos utilizados;
 - (v) adotar cautelas quanto à confidencialidade das informações acessadas, evitando exposição de telas, documentos ou dados institucionais em ambientes inadequados; e
 - (vi) comunicar imediatamente à SETIC qualquer incidente de segurança, perda, dano, comportamento anômalo de sistemas ou suspeita de acesso indevido.
6. Cumpre ainda registrar que, nos termos da regulamentação institucional aplicável ao teletrabalho, incumbe ao próprio agente público assegurar que o ambiente físico e tecnológico utilizado para a execução das atividades laborais atende às condições mínimas de segurança da informação, assumindo responsabilidade direta pela adequada utilização dos recursos tecnológicos e pela proteção dos dados institucionais acessados no exercício de suas atribuições (Resolução nº 305/2019).
7. Adicionalmente, o exercício das atividades em regime remoto deverá ocorrer em ambiente privado, adequado e compatível com a natureza das funções desempenhadas, de modo a assegurar a preservação da confidencialidade das informações institucionais, a integridade dos

sistemas corporativos e a autonomia funcional do agente público no desempenho de suas atribuições.

8. Nesse contexto, não se revela compatível com as exigências institucionais de segurança da informação, independência funcional e prevenção de conflitos de interesses a realização das atividades laborais em ambientes que mantenham vínculo direto com atividades privadas potencialmente relacionadas ao campo de atuação do Tribunal de Contas, tais como escritórios profissionais, empresas de consultoria, organizações que mantenham relação institucional com a Administração Pública ou outros espaços que possam suscitar situação de conflito de interesses real, potencial ou aparente (Resolução nº 433/2024).

9. Assim, o agente público deverá assegurar que o local escolhido para a execução do teletrabalho não exponha dados institucionais, sistemas corporativos ou rotinas administrativas a terceiros estranhos à Administração, nem permita circunstâncias que possam comprometer a imparcialidade, a autonomia funcional ou a percepção de integridade no exercício das atribuições públicas.

10. Nessa perspectiva, o ambiente utilizado para o teletrabalho não poderá expor dados institucionais, sistemas corporativos ou comunicações internas à visualização, acesso ou influência de terceiros estranhos à Administração, devendo o agente público adotar todas as cautelas necessárias para prevenir situações que possam comprometer a segurança da informação, a independência técnica do exercício funcional ou a percepção de integridade institucional.

11. Tal exigência também se orienta pela necessidade de prevenir circunstâncias que possam favorecer o compartilhamento indevido de informações institucionais ou gerar potenciais situações de conflito de interesses, incompatíveis com os deveres funcionais e com as políticas de integridade e governança desta Corte de Contas.

12. Nesse sentido, o acesso remoto aos sistemas do Tribunal será viabilizado por meio das soluções tecnológicas disponibilizadas pela SETIC — como ambientes virtuais seguros (VDI) ou conexões por rede privada virtual (VPN) com autenticação reforçada — cabendo ao usuário observar integralmente as orientações técnicas e boas práticas de segurança estabelecidas pela área responsável.

13. Importa assinalar, ainda, que as medidas ora reafirmadas não possuem caráter meramente recomendatório, constituindo deveres funcionais diretamente vinculados às políticas institucionais de governança, integridade e segurança da informação do Tribunal.

14. Assim, eventual negligência, imprudência ou descumprimento das diretrizes de segurança que resulte em exposição indevida de informações, comprometimento de sistemas institucionais ou vulnerabilização dos ativos informacionais da Corte poderá ensejar a apuração de responsabilidade administrativa individual, sem prejuízo de outras medidas cabíveis, nos termos das normas disciplinares e das políticas corporativas de segurança da informação vigentes.

15. A observância rigorosa dessas cautelas constitui medida essencial para a preservação da integridade dos sistemas institucionais, da confidencialidade das informações sob custódia deste Tribunal e da continuidade segura das atividades institucionais durante o período de trabalho remoto.

16. A Corregedoria Geral acompanhará o cumprimento dessas diretrizes sob a perspectiva orientativa e preventiva, reforçando a importância da atuação responsável, diligente e comprometida de cada agente público na proteção dos interesses institucionais e na consolidação da cultura de integridade e segurança da informação no âmbito desta Corte de Contas.

17. Diante o exposto, determino a expedição de memorando-circular a todas as unidades deste Tribunal cujos servidores e colaboradores estejam submetidos, temporariamente, ao regime de teletrabalho em razão das intervenções estruturais realizadas no edifício-sede, para ciência formal e estrita observância das diretrizes de segurança da informação, integridade e prevenção de conflitos de interesses consignadas nesta decisão.

18. Ciência à Presidência e a Secretaria de Tecnologia da Informação (SETIC).

19. Cumpra-se. Para tanto, expeça-se o necessário.

Gabinete da Corregedoria Geral, datado e assinado eletronicamente.

Conselheiro **PAULO CURI NETO**
Corregedor-Geral



Documento assinado eletronicamente por **PAULO CURI NETO, Conselheiro**, em 06/03/2026, às 11:17, conforme horário oficial de Rondônia, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#) e do art. 3º da [Instrução Normativa n. 84/2025/TCE-RO](#).



A autenticidade deste documento pode ser conferida no site <https://sei.tzero.tc.br/validar>, informando o código verificador **1018248** e o código CRC **140E9CDC**.

Referência: Processo nº 001808/2026

SEI nº 1018248

Av. Presidente Dutra, nº 4229 - Bairro Olaria - Porto Velho/RO - CEP 78902-030 - Telefone: (69) 3609-6504 - www.tzero.tc.br