** Publicada no DOETC/MS nº 3910, de 22 de novembro de 2024, páginas 9-15.*

# RESOLUÇÃO TCE-MS Nº 237, DE 21 DE NOVEMBRO DE 2024.

*Dispõe sobre a Política de Controle de Acesso a Dados e Informações do Tribunal de Contas do Estado de Mato Grosso do Sul (PCADI/TCE-MS) e dá outras providências.*

**O PRESIDENTE DO TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO DO SUL,** com fundamento no art. 9º, inciso I, da Lei Complementar n. 160, de 2 de janeiro de 2012, e tendo em vista o disposto no art. 74, § 2º do Regimento Interno, aprovado pela Resolução TCE/MS n. 98, de 5 de dezembro de 2018;

Considerando a importância de aprimorar e sistematizar a política e as práticas institucionais relacionadas à segurança da informação, as quais contribuem para assegurar o suporte necessário ao pleno exercício das funções do TCE-MS;

Considerando o Decreto Federal n.º 11.856/2023 que estabelece os objetivos estratégicos que visam nortear as ações planejadas do País em segurança cibernética, e representam macrodiretrizes basilares para que o setor público, o setor produtivo e a sociedade possam usufruir de um espaço cibernético resiliente, confiável, inclusivo e seguro;

Considerando os termos da Resolução Administrativa TC-MS n.º 100/2009, que em seu art. 18, instituiu o Comitê de Segurança da Informação (CSI), no âmbito do Tribunal de Contas do Estado de Mato Grosso do Sul, com o objetivo de estabelecer diretrizes e propor políticas, normas e procedimentos gerais relacionados à gestão informacional e do conhecimento;

Considerando a necessidade de implementação, manutenção e monitoramento do Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados (PCGSIPD) do TCE-MS, para assegurar compliance e conformidade com as leis e regulamentações aplicáveis à segurança da informação e à privacidade, inclusive, às relacionadas ao tratamento de dados pessoais;

Considerando a necessidade de aprimorar os mecanismos de proteção e de segurança das informações, ativos e serviços de tecnologia da informação do TCE-MS, bem como de adequar o arcabouço normativo em função de novos paradigmas, como armazenamento em nuvem e trabalho remoto;

Considerando o advento da Lei Federal n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal;

Considerando o disposto nos incisos X e XII do caput do art. 5º da Constituição Federal e na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);

Considerando as boas práticas preconizadas pelas normas ABNT NBR ISO/IEC 27003:2011, 27005:2011, 27001:2013, 27002:2013, 27014:2013, 27004:2017, 29100:2020, 27701:2020, 16167:2013, 31000:2018, 27701:2019 e 27003:2020;

**RESOLVE *AD REFERENDUM:***

## CAPÍTULO I
## DAS DISPOSIÇÕES GERAIS

**Art. 1º** Por meio desta Resolução, fica instituída a Política de Controle de Acesso aos Dados e Informações do Tribunal de Contas do Estado de Mato Grosso do Sul - TCE-MS (PCADI/TCE-MS).

**Art. 2º** A PCADI/TCE-MS define as diretrizes para delimitar o acesso à informação e aos Recursos de Tecnologia da Informação (RTI), estabelecendo controles de acesso, garantindo a segurança e níveis adequados de proteção, englobando os seguintes aspectos:

I- contas de usuários (identificação);

II- autenticação e autorização;

III- interação com dados físicos e digitais;

IV- controles rígidos a visitantes.

Parágrafo único. Esta norma integra a Política Corporativa de Segurança da Informação do Tribunal de Contas do Estado de Mato Grosso do Sul (POSIC/TCE-MS).

## CAPÍTULO II
## DA IDENTIFICAÇÃO DE USUÁRIOS E DAS CONTAS DE ACESSO

**Art. 3º** São usuários, quando autorizados, dos Recursos de Tecnologia da Informação, produzidas ou custodiadas do Tribunal de Contas do Estado de Mato Grosso do Sul (RTI/TCE-MS):

I- interno: membro ou servidor ativo;

II- inativo: membro emérito, servidor inativo ou pensionista;

III- colaborador: prestador de serviço terceirizado, estagiário, aprendiz ou qualquer outro;

IV- externo: pessoa que utiliza serviços digitais do TCE-MS de forma identificada e que não se enquadre nas definições contidas nos incisos I, II e III deste artigo; e

V- visitante: pessoa que não se enquadre nas definições dispostas nos incisos anteriores, com acesso temporário, somente à internet disponibilizada no âmbito do TCE-MS.

**Art. 4º** Cada usuário possuirá uma única conta para acesso aos RTI/TCE-MS, exceto nos casos explicitamente definidos e autorizados pelo Setor de Tecnologia da Informação (STI).

**Art. 5º** As contas de usuários são pessoais e intransferíveis, de responsabilidade exclusiva do respectivo titular e os limites de sua autorização de acesso não podem ser estendidos a terceiros.

Parágrafo único. As contas de usuários serão utilizadas para registro de operações passíveis de monitoramento ou não, realizadas pelos respectivos titulares.

**Art. 6º** As atividades de criação, atualização e revogação de conta de usuário para acesso aos RTI/TCE-MS serão realizadas pelo STI, com base nas informações prestadas:

I – pela Setor de Gestão de Pessoas, quando se tratar de servidor ativo, inativo ou pensionista;

II – pela Presidência, quando se tratar dos membros, corpo diretivo e colaboradores;

Parágrafo único. A definição e divulgação dos procedimentos a serem executados com vistas à criação, atualização e à revogação de contas de usuários serão promovidos pelo STI.

**Art. 7º** A concessão e o uso de direitos de acesso privilegiado em sistemas, infraestrutura de redes e demais recursos tecnológicos, serão restritos e controlados pelo STI, que deverá:

I- manter um processo de autorização formal, bem como o registro de todas as contas de usuários, os tipos de privilégios concedidos e associados a cada sistema ou processo;

II- assegurar que direitos de acesso privilegiados não sejam concedidos, até que todo o processo de autorização esteja finalizado;

III- garantir que os direitos de acesso privilegiados sejam atribuídos a uma Identificação de Usuário (ID) diferente daquelas usadas nas atividades normais do negócio;

IV- acompanhar para que as atividades normais do negócio não sejam desempenhadas usando ID privilegiado;

V- analisar criticamente, em intervalos regulares, se as competências dos usuários com direitos de acesso privilegiado estão alinhadas com as suas obrigações, no âmbito do TCE-MS; e

VI- estabelecer e manter procedimentos específicos para evitar o uso não autorizado do ID de usuário de administrador genérico, de acordo com as capacidades de configuração dos sistemas.

Parágrafo único. As senhas associadas às contas com acesso privilegiado, devem ser compostas usando uma quantidade mínima de 15 (quinze) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais.

**Art. 8º** Será permitida, em caráter excepcional e temporária, a conta de uso coletivo, restrita à finalidade que justificar sua criação, destinada para usuários em treinamento ou evento, bem como nos casos em que não seja considerado viável o uso de conta individual.

§1º A criação de conta de uso coletivo para finalidade prevista no caput será solicitada, para o STI, que analisará as justificativas apresentadas e autorizará ou não o atendimento do pedido ou ainda poderá apresentar solução alternativa.

§2º A revogação da conta de uso coletivo prevista neste artigo, será feita imediatamente após a expiração do prazo definido ou antes, caso o demandante comunique não ser mais necessária.

## CAPÍTULO III
## DA AUTENTICAÇÃO E DA AUTORIZAÇÃO

**Art. 9º** A autenticação de contas no ambiente de RTI/TCE-MS será feita, ao menos, por meio de mecanismo de usuário e senha, atendendo a requisitos mínimos da Política de Senha, estabelecidos pela Resolução TCE-MS n.° 195, de 09 de agosto de 2023.

**Art. 10** Sempre que possível, deverá ser adotada a autenticação em dois fatores para acesso a quaisquer serviços ou soluções de TI, exceto nos casos definidos e justificados pelo STI.

§1° Enquanto estiver autenticado, o usuário não deverá se afastar do equipamento sem o bloquear para evitar eventuais acessos de usuários não autorizados;

§2° O mecanismo de autenticação automática (auto login) deverá ser desabilitado nos recursos de TI.

§3° Conta de usuário não será empregada em processos de autenticação em serviços de sistema, incluindo rotinas de agendamento de tarefas.

§4° Poderão ser requeridos, como meio alternativo de autenticação, mecanismos de segurança adicionais como certificação digital e biométrica.

**Art. 11** O controle de acesso à nuvem do TCE-MS poderá ser feito por intermédio de serviços de diretórios localizados na própria nuvem, com sincronização unidirecional de contas e privilégios, atualizadas a partir da rede do TCE-MS, inclusive no tocante à troca de senhas. Parágrafo único. A sincronização não envolverá contas administrativas, as quais serão mantidas na rede do TCE-MS, exceto as definidas pelo STI.

**Art. 12** A autorização de acesso aos RTI/TCE-MS respeitará o princípio do menor privilégio e a necessidade de conhecer, bem como observará as seguintes diretrizes:

I - a definição da permissão ou revogação de acesso aos recursos de TI, será motivada e autorizada pelo dirigente da unidade em que o usuário presta serviço mediante abertura de chamado ao STI;

II - a concessão de acesso será preferencialmente automatizada, sendo realizada e atualizada de acordo com os atributos do usuário, a exemplo da unidade de lotação, da função, entre outros;

Parágrafo único. É responsabilidade do dirigente da unidade comunicar ao STI no caso de mudança de lotação de usuário, mediante abertura de chamado, solicitando que as permissões que foram concedidas sejam revogadas, exceto se houver a necessidade de continuidade do serviço.

**Art. 13** O bloqueio de conta de usuário poderá ser realizado conforme critérios de risco de segurança da informação e privacidade definidos pelo CSI, além das situações abaixo identificadas:

I- conta sem uso, por período igual ou superior a 30 (trinta) dias, ressalvadas as contas de usuários externos, cujo período de inatividade deverá ser superior a 03 (três) anos, com possibilidade de exclusão definitiva;

II- quando o servidor ativo não estiver em efetivo exercício por prazo igual ou superior a 15 (quinze) dias, em função de licenças e/ou afastamentos previstos na legislação, mediante informações encaminhadas pela SGP; ou

III- nos casos de envio de alerta para a unidade de Infraestrutura e Segurança da Informação (USIN) e de habilitação de mecanismo de verificação por desafio cognitivo, em função de erros sucessivos de autenticação, a fim de mitigar riscos de segurança decorrentes de tentativas de comprometimento da conta de usuário.

§1° O bloqueio de conta, a que se refere o inciso I, poderá ser realizado automaticamente, observados os procedimentos estabelecidos pelo STI e poderá ser revogado mediante solicitação do usuário.

§2° Vencido o prazo informado no inciso II, a conta será liberada.

## CAPÍTULO IV
## DAS RESPONSABILIDADES

**Art. 14** São responsabilidades dos usuários relacionadas ao emprego de credenciais de acesso aos RTI/TCE-MS:

I- salvaguardar senhas, certificados digitais e quaisquer outros meios empregados na autenticação da RTI/TCE-MS;

II- proceder à troca periódica de senhas;

III- revisar, periodicamente, privilégios recebidos e solicitar a revogação dos considerados não mais necessários;

IV- reportar ao CSI (Comitê de Segurança da Informação) e colaborar para o tratamento de incidentes de segurança que tiver conhecimento;

V - observar orientações do TCE-MS quanto às boas práticas e às configurações específicas de segurança da informação e proteção de dados pessoais;

VI - usar, em estrito interesse e razões de serviço, os dispositivos, equipamentos, sistemas e serviços colocados à sua disposição para o exercício funcional; e

VII - observar o disposto na POSIC-TCE-MS, quanto à salvaguarda de informações produzidas ou custodiadas pelo Tribunal, bem como à proteção dos RTI-TCE-MS.

**Art. 15** Todo agente público e colaborador que ingressar no TCE-MS deve assinar um termo de confidencialidade e responsabilidade para ter acesso às informações e aos recursos de Tecnologia da Informação (TI), sendo de responsabilidade da SGP, o armazenamento seguro do termo, em meio físico ou eletrônico.

Parágrafo único. No caso de prestador de serviço ou fornecedor que necessite acesso às informações ou aos recursos de TI, o gestor ou fiscal do contrato ficará responsável por recolher a assinatura no termo de confidencialidade e responsabilidade, e de seu arquivamento no respectivo processo de contratação.

**Art. 16** São responsabilidades das USIN e do CSI, como administradoras do serviço de autenticação dos RTI/TCE-MS:

I - garantir a disponibilidade de serviços de Controle de Acesso (CA), de acordo com os níveis definidos;

II - definir os perfis e permissões de acesso para as funcionalidades e informações das soluções e serviços de TI;

III - definir e revisar, periodicamente, as regras para conceder, revogar ou modificar perfis e permissões de acesso a usuários;

IV - implantar e manter atualizados mecanismos e procedimentos de proteção contra ataques externos e internos relacionados ao CA, incluindo mecanismos de validação de senhas;

V - gerenciar contas configuradas;

VI - impedir a transmissão de senhas em texto claro pela rede e armazená-las com criptografia;

VII - implementar o Protocolo de Transferência de Hipertexto Seguro (HTTPS) e regras de identificação e autorização criptografadas, impedindo o tráfego e o armazenamento de senhas em texto claro em todos os sistemas web e portais do TCEMS;

VIII - armazenar dados de usuário e senha apenas em Sistemas Gerenciadores de Banco de Dados (SGBDs);

IX - realizar triagem, análise, notificação e resposta a incidentes de segurança da informação relacionados aos serviços de CA;

X - realizar identificação periódica e notificação de vulnerabilidades, bem como monitorar a aplicação de correções (patches) em sistemas e serviços de CA; e

XI - executar, manter e restaurar cópias de segurança (backup) de informações disponíveis em serviços de CA.

**Art. 17** O STI deverá garantir e manter o acesso ao Data Center do TCE-MS restrito e autorizado, somente aos servidores lotados na USIN e o Diretor da STI.

Parágrafo único. As pessoas não contempladas no caput só poderão ter acesso se acompanhadas pelos servidores autorizados.

**Art. 18** O monitoramento por Circuito Fechado de Televisão (CFTV) deve ser implementado e mantido, nos perímetros de acesso ao(s) Data Center(s) do TCE-MS.

Parágrafo único. O tempo de retenção das imagens gravadas pelo sistema de CFTV mencionadas no caput deve ser de, no mínimo, 03 (três) meses.

## CAPÍTULO XII
## DAS DISPOSIÇÕES FINAIS

**Art. 19** O presente normativo utilizará o Glossário de termos do Anexo I e, ainda, o Glossário constante da POSIC/TCE-MS para promover compreensão comum e consistente de conceitos, em função da natureza específica do tema.

**Art. 20** A violação ou a inobservância aos dispositivos desta Resolução poderá ser considerada incidente de segurança institucional, patrimonial ou da informação e implicar, isolada ou cumulativamente, nas sanções previstas na POSIC/TCE-MS e/ou em políticas complementares, bem como civis e penais, nos termos da legislação pertinente, assegurados aos envolvidos o contraditório e a ampla defesa.

**Art. 21** A unidade provedora de TI adotará as medidas necessárias para operacionalizar o disposto nesta norma.

**Art. 22** A revisão desta PCA/TCE-MS poderá ocorrer sempre que houver mudanças significativas com impacto nos processos ou requisitos de segurança da informação e privacidade, devendo, obrigatoriamente, ser realizada no máximo a cada 02 (dois) anos, de modo a atualizá-la.

**Art. 23** O STI poderá, sem aviso prévio, bloquear, restringir acesso ou solicitar imediatamente a troca de senhas de qualquer conta de usuário com comportamento considerado suspeito e que possa causar risco de segurança ao ambiente tecnológico e de negócio do TCE-MS.

**Art. 24** Os casos omissos serão resolvidos pelo Comitê da Segurança da Informação – CSI.

**Art. 25** A PCA/TCE-MS será administrada pelo Comitê de Segurança da Informação - CSI, instituído pela Resolução Administrativa TCE/MS nº 100 de 18 de novembro de 2009.

**Art. 26** Esta Resolução entrará em vigor na data de sua publicação.

Campo Grande, 21 de novembro de 2024.

CONSELHEIRO JERSON DOMINGOS
Presidente

**Alessandra Ximenes**
Chefe da Diretoria das Sessões dos Colegiados

**ANEXO I DA RESOLUÇÃO nº xxx, de xxx de xxx de 2024.**

## APRESENTAÇÃO

Este Glossário fornece definições de termos, aplicáveis à Política de Controle de Acesso do Tribunal de Contas do Estado de Mato Grosso do Sul, para promover uma compreensão comum e consistente de conceitos sobre o tema. É complementar ao Glossário da Política Corporativa de Segurança da Informação (PCSI/TCE-MS).

## GLOSSÁRIO

**A**

**Acesso privilegiado:** capacidade de um usuário ou sistema acessar recursos, informações ou funcionalidades que estão fora do alcance da maioria dos outros usuários ou sistemas. Deve ser concedido apenas a usuários confiáveis que precisem dele para realizar suas funções, como administradores de sistemas, de redes e de segurança.

**Acesso remoto:** ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário. Esse acesso permite a visualização da tela do usuário.

**Ativos:** qualquer dispositivo de software ou hardware que agrega valor ao negócio e compõe a infraestrutura de rede de dados do Tribunal, assim como também os locais onde se encontram esses dispositivos.

**C**

**CFTV (Circuito Fechado de Televisão):** técnica de segurança que usa câmeras de vigilância para monitorar e gravar imagens de um determinado local.

**Conta de uso coletivo:** contas temporárias, com duração equivalente ao período necessário para realizar atividades no TCE-MS, com prazo de expiração pré-definido pelas unidades provedoras de TI.

**Controle de acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso aos recursos de tecnologia da informação.

**D**

**Data center:** instalação física centralizada onde se encontram computadores corporativos, rede, armazenamento e outros equipamentos de TI que dão suporte às operações de negócios.

**I**

**Informação:** conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado.

**L**

**Log ou registro de auditoria:** registro de eventos relevantes em um dispositivo ou sistema computacional.
Login: ter acesso a algo no meio digital.

**Logoff:** procedimento seguro de saída do sistema.

**Logon:** procedimento seguro de entrada no sistema.

**M**

**Medidas:** medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo.

**N**

**Nuvem:** serviço hospedado fora do ambiente próprio que contempla toda a necessidade tecnológica de servidor, armazenamento, backup e alta disponibilidade.

**P**

**Perfil:** conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso.

**Prestador de serviço:** pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que devem receber credencial diferenciada de acesso.

**Proprietário da informação:** membro ou servidor do TCE-MS que tenha a guarda das informações produzidas ou que estejam sob responsabilidade do setor onde estão lotados. São responsabilidades do proprietário da informação atribuir os níveis de classificação que uma informação requer, reclassificar esta informação quando necessário e autorizar o acesso à informação aos usuários do TCE-MS.

**S**

**Segurança da informação:** proteção da informação contra ameaças a sua confidencialidade, integridade, disponibilidade e autenticidade, para minimizar riscos, garantir a eficácia das ações do negócio e preservar a imagem do TCE-MS.
Sigilo: segredo de conhecimento restrito a pessoas credenciadas; proteção contra revelação não autorizada.

**T**

**Termo de responsabilidade:** termo assinado pelo usuário, comprometendo-se em manter a confidencialidade acerca de assuntos classificados como sigilosos dos quais tenha tomado conhecimento ou tido acesso em razão de seu ofício no TCE-MS, zelando pela proteção dos documentos, materiais, áreas e sistemas de informação, sob sua responsabilidade, e usando, em estrito interesse e razões de serviço, os dispositivos, equipamentos e sistemas colocados à sua disposição para o exercício funcional.

**U**

**Usuário:** membro, servidor, prestador de serviço ou fornecedor do TCE-MS que obteve

autorização do Proprietário da Informação pela área interessada para acesso aos Ativos de Informação, formalizada por meio da assinatura do Termo de Responsabilidade e/ou pedido de concessão de acesso.

**Usuário colaborador:** prestador de serviço terceirizado, estagiário ou qualquer outro colaborador do Tribunal que tenha acesso, de forma autorizada, às informações produzidas ou custodiadas por esta Corte.

**Usuário externo:** pessoa que utiliza serviços digitais do TCE-MS, de forma identificada.

**Usuário inativo:** membro emérito, servidor inativo ou pensionista do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo TCE-MS.

**Usuário interno:** membro ou servidor ativo que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo TCE-MS.

**Usuário visitante:** pessoa com acesso temporário, somente à internet no âmbito desta Corte de Contas.