TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO DO SUL
R. Desembargador Leão Neto do Carmo, 23 - Bairro Parque dos Poderes - CEP 79037-100 - Campo Grande - MS

RESOLUÇÃO Nº 861

Institui norma para a Gestão de Identidade e o Controle de Acesso Físico e Lógico ao ambiente cibernético do Tribunal Regional Eleitoral de Mato Grosso do Sul.

O egrégio **TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO DO SUL**, no uso de suas atribuições legais e com fundamento no art. 42, incisos X e XII, de seu Regimento Interno (Resolução n. 801/2022), bem como em conformidade com os elementos constantes do Processo Administrativo SEI nº 6403-62.2024.6.12.8000 e, ainda,

Considerando os princípios da igualdade e da legalidade a serem observados pelos candidatos que participarem das eleições, e visando resguardar a vontade dos eleitores no exercício pleno de sua cidadania;

Considerando a necessidade de definir processos de gestão de identidade e controle de acesso físico e lógico aos ativos de informação;

Considerando que a segurança da informação e a proteção de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos;

Considerando que o acesso à informação, assim como aos recursos de processamento das informações e aos processos de negócios, deve ser controlado com base nos requisitos de negócio e da segurança da informação;

Considerando a Resolução CNJ n.º 396, de 7 de junho de 2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

Considerando a Resolução TSE n.º 23.644, de 1º de julho de 2021, que instituiu a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

Considerando a NC 07/IN01/DSIC/GSIPR, de 15 de julho de 2014, que estabeleceu diretrizes para implantação de controles de acesso relativos à segurança da informação e das comunicações na Administração Pública Federal;

Considerando as boas práticas de segurança da informação e privacidade previstas nas normas da Associação Brasileira de Normas Técnicas - ABNT ISO/IEC 27001 e ABNT ISO/IEC 27002, complementadas pela norma ABNT NBR ISO/IEC 27701;

Considerando a Resolução TRE/MS n.º 822, 8 de abril de 2024, que implementa, no âmbito do TRE/MS, a PSI da Justiça Eleitoral estabelecida pela Resolução TSE nº 23.644/2021;

Considerando, ainda, as recomendações do Acórdão n.º 1.603/2008-TCU, item 9.1.3, sobre a importância dos controles de acesso,

R E S O L V E:

Capítulo I

DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a norma de Gestão de Identidade e Controle de Acesso Físico e Lógico relativa à segurança da informação e comunicação no âmbito do Tribunal Regional Eleitoral de Mato Grosso do Sul.

Art. 2º Esta norma integra a Política de Segurança da Informação da Justiça Eleitoral, estabelecida pela Resolução TSE n.º 23.644/2021.

Capítulo II

DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para efeitos desta norma, consideram-se os termos e definições previstos na Portaria DG/TSE n.º 444, de 8 de julho de 2021, aplicando-se, de forma subsidiária, aqueles estabelecidos no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República.

Capítulo III

DOS PRINCÍPIOS

Art. 4º O controle de acesso é regido pelos seguintes princípios:

I - necessidade de saber: as(os) usuárias(os) deverão ter acesso somente às informações necessárias ao desempenho de suas tarefas;

II - necessidade de uso: as(os) usuárias(os) deverão ter acesso apenas aos ativos (equipamentos de TI, sistemas, aplicações, procedimentos, salas) necessários ao desempenho de suas tarefas;

III - privilégio mínimo: deverão ser conferidos apenas os privilégios necessários para que a(o) usuária(o) realize a sua função na organização; e

IV - segregação de funções: consiste na separação das funções desempenhadas no controle de acesso, por exemplo, pedido de acesso, autorização de acesso e administração de acesso.

Art. 5º As diretrizes de controle de acesso devem ser apoiadas por procedimentos documentados, com responsabilidades e papéis definidos.

Capítulo IV

DO ESCOPO E DO ÂMBITO DE APLICAÇÃO

Art. 5º O objetivo desta Norma de Gestão de Identidade e Controle de Acesso Físico e Lógico relativos à segurança da informação e comunicação consiste em:

I - estabelecer diretrizes para implantação de controles de acesso físico e lógico; e

II - assegurar a confidencialidade, integridade e disponibilidade dos ativos de informação e comunicação sob a responsabilidade deste Tribunal.

Art. 6º Este normativo se aplica às(aos) magistradas(os), servidoras(es), requisitadas(os), e cedidas(os), e, desde que previamente autorizadas(os), colaboradoras(es) internos e externos, estagiárias(os), ocupantes de cargo em comissão sem vínculo efetivo, membras(os) do Ministério Público e quaisquer outras pessoas que se encontrem a serviço da Justiça Eleitoral e fazem uso ou tenham acesso aos ativos de informação e de processamento da Justiça Eleitoral.

§ 1º Os contratos celebrados pelo Tribunal com entidades privadas ou parcerias celebradas com outros órgãos públicos, acordos de cooperação de qualquer tipo, convênios e termos congêneres que fazem uso dos ativos de informação e de processamento no âmbito da Justiça Eleitoral, deverão atender os requisitos desta política, bem como as normas referentes à proteção de dados pessoais.

§ 2º Os destinatários desta norma, relacionados no *caput*, são corresponsáveis pela segurança da informação e comunicação, de acordo com os preceitos estabelecidos neste normativo.

Capítulo V

DO CONTROLE DE ACESSO FÍSICO

Seção I

Das Definições Gerais

Art. 7º Fica estabelecido, por meio deste normativo, que as instalações de processamento e armazenamento da informação (datacenter) e das demais áreas que contenham informações críticas ou sensíveis ao Tribunal serão tratados como perímetro de segurança física devendo receber proteção adequada e compatível com a importância dos ativos de informação.

Art. 8º As instalações do datacenter devem atender, no mínimo, às seguintes diretrizes:

I - paredes fisicamente sólidas, sem brechas nem pontos por onde possa ocorrer uma invasão, portas externas adequadamente protegidas por mecanismos de controle contra acesso não autorizado, sem janelas ou, na impossibilidade, com janelas com proteção externa;

II - videomonitoramento de sua área interna e de seu perímetro;

III - controle de acesso físico às áreas e instalações, sob a responsabilidade da Secretaria de Tecnologia da Informação, utilizando-se dos mecanismos necessários para o controle e registro de data e hora de todas as entradas e saídas, sejam de servidoras(es), visitantes ou prestadores de serviço, permitindo-lhes o acesso, desde que previamente autorizados;

IV - adotar mecanismos de autenticação de multifator, acesso biométrico ou fechadura por senha, para as instalações de processamento, armazenamento e comutação de dados, restritas ao pessoal autorizado;

V - portas corta-fogo com sistema de alarme, monitoradas, que funcionem de acordo com os códigos locais, para minimizar os riscos de ameaças físicas potenciais;

VI - sistemas para detecção de intrusos em todas as portas externas e janelas acessíveis;

VII - instalações de processamento e armazenamento das informações que sejam projetadas para minimizar os riscos de ameaças físicas potenciais, tais como fogo, inundação, enchente, vibrações danosas, explosão, manifestações civis, ataques maliciosos, fumaça, furtos;

VIII - edifícios que sejam dotados de proteção contra raios e que, em todas as linhas de entrada de força e de comunicações, tenham filtros de proteção contra raios;

IX - alimentações alternativas de energia elétrica e telecomunicações, com rotas físicas diferentes;

X - iluminação e comunicação de emergência; e

XI - sistema de controle de temperatura e umidade com recurso de emissão de alertas.

Art. 9º As diretrizes para proteção das demais áreas que contenham informações críticas ou sensíveis que não estejam armazenadas no datacenter devem ser estabelecidas pela Comissão de Segurança da Informação, observadas as legislações vigentes.

Art. 10. As regras e processos associados ao controle de acesso devem ser implementadas considerando a consistência entre os direitos de acesso e as necessidades e requisitos de segurança de perímetro físico.

Seção II

Dos Equipamentos de Processamento e Armazenamento

Art. 11. Para evitar perdas, danos, furtos ou comprometimento de ativos e interrupção das operações da organização, o Tribunal deve observar as seguintes diretrizes:

I - adotar controles para minimizar o risco de ameaças físicas potenciais e ambientais, como furto, incêndio, explosivos, fumaça, água, poeira, vibração, efeitos químicos, interferência com o suprimento de energia elétrica, interferência com as comunicações, radiação eletromagnética e vandalismo;

II - verificar se os suprimentos de energia elétrica, telecomunicações, água, gás, esgoto, calefação/ventilação e sistema de ar-condicionado estejam em conformidade com as especificações do fabricante do equipamento e com os requisitos legais da localidade;

III - adotar controles para evitar a retirada de equipamentos do Tribunal sem prévia autorização da unidade competente, conforme regulamentação específica; e

IV - utilizar, sempre que possível, racks que disponham de fechaduras com chave ou mecanismo semelhante, garantindo que apenas a(s) equipe(s) responsáveis pelos ativos instalados nos racks tenham acesso físico a eles.

Seção III

Da Segurança do Cabeamento

Art. 12. O cabeamento de energia elétrica e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação, interferência ou danos, conforme as seguintes diretrizes:

I - as linhas de energia elétrica e de telecomunicações que entram nas instalações de processamento da informação devem ser subterrâneas ou ficar abaixo do piso, sempre que possível, e devem atender aos requisitos mínimos de proteção; e

II - os cabos de energia elétrica devem ser segregados dos cabos de comunicação, para evitar interferências eletromagnéticas.

Seção IV

Da Manutenção Externa dos Equipamentos

Art. 13. A manutenção dos equipamentos de processamento de informações deve seguir as seguintes diretrizes:

I - ser realizada somente por pessoal de manutenção identificado e autorizado;

II - o provedor de serviço deverá informar a lista de todas(os) as(os) técnicas(os) autorizadas(os) para acesso às dependências do Tribunal para realização da manutenção. O provedor deve encaminhar notificação ao Tribunal sempre que houver dispensa de colaborador(a) mediante encerramento de contratos ou acordos, para revogação imediata de credenciais/direitos de acesso;

III - devem ser incluídas cláusulas nos contratos com previsão da responsabilidade do provedor de serviço em manter a lista de colaboradoras(es) atualizada.

IV - deve ser mantido o registro de todas as falhas - suspeitas ou reais - e de todas as operações de manutenção preventiva e corretiva realizadas;

V - devem ser eliminadas as informações sensíveis do equipamento, quando possível, ou tratar de forma alternativa os riscos de sua exposição; e

VI - o equipamento deverá ser inspecionado, após a manutenção, para garantir que não foi alterado indevidamente e que está em perfeito funcionamento.

Seção V

Da Reutilização ou Descarte Seguro dos Equipamentos ou dos Equipamentos em Prova de Conceito

Art. 14. Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes da reutilização ou descarte, para assegurar que dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança.

Parágrafo único. As mídias que contenham informações com acesso restrito de propriedade intelectual devem ser apagadas fisicamente, bem como as informações devem ser destruídas, apagadas ou sobrescritas por meio de técnicas que tornem as informações originais irrecuperáveis.

Capítulo VI

DO CONTROLE DE ACESSO LÓGICO

Seção I

Do Gerenciamento de Acesso Lógico

Art. 15. O acesso aos sistemas de informação será assegurado, unicamente, à(ao) usuária(o) devidamente identificada(o) e autorizada(o).

Parágrafo único. As(Os) gestoras(es) dos ativos devem determinar regras apropriadas de controle de acesso, direitos de acesso e restrições para papéis específicos das(os) usuárias(os) terem acesso aos ativos, com nível de detalhe e rigor de controle que reflitam os riscos de segurança da informação associados, observada a consistência entre os direitos de acesso e as políticas de classificação da informação.

Art. 16. A concessão e a revogação de acesso serão implementadas por meio de um processo formal, preferencialmente automatizado, com estabelecimento de responsáveis pela solicitação, administração, concessão, bloqueio e revogação.

§ 1º Compete às(aos) proprietárias(os) de todos os tipos de ativos estabelecer regras de concessão, bloqueio e revogação de acesso aos ativos para as(os) usuárias(os), levando em conta as políticas, princípios e normas de controle de acesso aplicáveis.

§ 2º Os acessos deverão ser retirados imediatamente após a revogação dos direitos ou o encerramento das atividades, contratos ou acordos, ou ajustados após qualquer mudança de atribuições.

§ 3º As contas deverão ser desabilitadas, em vez de excluídas, para preservação de trilhas de auditoria.

Art. 17. A criação de nomes de usuária(o) e de contas de e-mail seguirá critérios padronizados pela Secretaria de Tecnologia da Informação.

Parágrafo único. A identificação da conta de e-mail (login) não poderá ser alterada, exceto quando ocorrer alteração do nome da(o) usuária(o), caso em que será necessária a manifestação expressa da(o) usuária(o) no interesse da referida modificação.

Art. 18. O modelo de controle de acesso será, preferencialmente, fundamentado no controle de acesso baseado em papéis (RBAC).

Art. 19. Deverá ser estabelecido e mantido atualizado um inventário de todas as contas gerenciadas, contendo data de início e término, incluindo:

I - contas de usuária(o) e de administradora(or); e

II - contas de serviço.

§ 1º O inventário das contas de usuária(o) e de administradora(or) deverá conter, no mínimo, o nome da pessoa, o nome de usuária(o) e a sua unidade de lotação, enquanto o das contas de serviço indicará ao menos a unidade gestora, as datas de revisão e o propósito.

§ 2º As contas deverão ser revisadas trimestralmente, pela unidade responsável, para avaliar se as contas ativas permanecem autorizadas.

Art. 20. A Secretaria de Tecnologia da Informação deverá manter inventário dos sistemas de autenticação do Tribunal, abrangendo os internos e aqueles hospedados em provedores remotos.

Art. 21. A Secretaria de Tecnologia da Informação deve considerar a revogação do direito de acesso de uma(um) usuária(o) às informações sensíveis ou aos ativos críticos do Tribunal, antes da ocorrência de alteração ou rescisão do contrato de emprego, ou tratar de forma alternativa os riscos associados aos acessos concedidos.

Seção II

Da Gestão de Identidades, do Acesso às Redes, Sistema Interno e Serviços de Rede

Art. 22. A gestão de contas internas e o controle de acesso se darão de forma centralizada, por meio de serviço de diretório.

Art. 23. As operações de criação de usuárias(os) da rede local serão solicitadas por meio de instrumento formal específico, observada a segregação de funções em todo o fluxo do gerenciamento de acesso, pelos seguintes agentes:

I - Secretaria de Gestão de Pessoas, chefia imediata da unidade de lotação da(o) usuária(o) ou ainda coordenadoria, secretaria ou assessoria a qual a unidade pertence, no caso de magistradas(os), servidoras(es) efetivas(os) e requisitadas(os), ocupantes de cargo em comissão sem vínculo efetivo e estagiárias(os); e

II - chefia imediata da unidade de lotação da(o) usuária(o), no caso de colaboradoras(es), estagiárias(os) e prestadoras(es) de serviços temporários.

Parágrafo único. Nos demais casos, será necessária a aprovação da Comissão de Segurança da Informação.

Art. 24. A chefia imediata da unidade de lotação da(o) usuária(o) deverá solicitar a atribuição de direitos de acesso aos recursos computacionais do Tribunal por meio da Central de Serviços de TI (Service Desk) da Secretaria de Tecnologia da Informação, informando os sistemas ou serviços de informação e o perfil de acesso que a(o) usuária(o) deve possuir.

§ 1º O perfil de acesso da(o) usuária(o) aos sistemas ou serviços de informação deve ser mantido restrito ao desempenho de suas atividades.

§ 2º A(O) gestora(or) do ativo de informação será responsável pela autorização do direito de acesso, que poderá ser operacionalizado por equipe técnica designada.

§ 3º Na análise da solicitação de acesso, a(o) gestora(or) do ativo deverá considerar também a consistência entre a classificação da informação e os direitos de acesso, bem como as normas e legislação vigentes.

§ 4º Estas autorizações devem estar documentadas, para fins de auditoria e levantamento periódico, visando à detecção de usuárias(os) com acesso indevido.

§ 5º A unidade responsável pelo cadastramento deverá estabelecer procedimentos para verificar a identidade de uma(um) usuária(o) antes de fornecer uma identidade lógica.

§ 6º Deverá ser estabelecido um perfil padrão para usuárias(os), ao qual todas(os) retornarão em caso de mudança de lotação ou qualquer outro motivo que leve à suspensão de suas atividades, antes que sejam solicitados novos perfis de acesso pela nova chefia.

§ 7º A lotação de uma(um) usuária(o) em uma unidade permite acesso à área específica de armazenamento de arquivos da unidade, bem como o recebimento de mensagens para o e-mail da mesma.

§ 8º Caso existam mensagens ou arquivos para os quais nem todos tenham acesso, deve-se criar grupo de distribuição de mensagens ou de permissão de acesso distinto do padrão da unidade.

§ 9º O procedimento de atribuição de acesso não deve admitir que a permissão seja efetivada antes que a autorização formal seja finalizada.

§ 10. A(O) usuária(o), uma vez cadastrada(o), deverá por meio do Termo de Responsabilidade de Acesso à Rede - ANEXO I, assumir o compromisso de:

I - declarar o conhecimento e aceitação dos termos da Política de Segurança da Informação do Tribunal Regional Eleitoral de Mato Grosso do Sul e a Política Geral de Privacidade e Proteção de Dados Pessoais do Tribunal Regional Eleitoral de Mato Grosso do Sul, normas e procedimentos complementares, não podendo a qualquer tempo alegar desconhecimento ou ignorância;

II - declarar estar ciente que os acessos realizados por meio da Rede do Tribunal à Internet, assim como o tráfego das mensagens de correio eletrônico institucional são passíveis de auditoria; e

III - manter a segurança e confidencialidade de sua senha, alterando a mesma sempre que existir qualquer indício de possível comprometimento, em intervalos regulares de tempo ou com base no número de acessos, a critério da Secretaria de Tecnologia da Informação.

Art. 25. A STI deve manter os registros de todos os eventos significativos sobre o uso e gestão de identidade de usuárias(os) e as informações de autenticação/acesso aos sistemas como, por

exemplo, falha de autenticação de logon no serviço de diretórios, reset de senhas de usuárias(os), desativação e exclusão de contas de usuárias(os) e computadores, dentre outros.

Art. 26. As(Os) usuárias(os) devem possuir identificação única e exclusiva para permitir relacioná-la às suas ações e responsabilidades.

§ 1º Não deverá ser realizado cadastro que possua identificação genérica, ou seja, o cadastro deve permitir a identificação unívoca da(o) usuária(o).

§ 3º As referidas contas de acesso são fornecidas exclusivamente para que as(os) usuárias(os) possam executar suas atividades laborais, com base nos princípios do menor privilégio ou privilégio mínimo, bem como na segregação de funções.

Art. 27. Identidades atribuídas a várias pessoas, (a exemplo de identidades compartilhadas) só serão permitidas quando forem necessárias por razões de negócios ou operacionais e devem estar sujeitas à aprovação e documentação dedicadas, mediante procedimento de atribuição de responsabilidades compartilhado pelas chefias imediatas e autorização da Comissão de Segurança da Informação.

Art. 28. Compete à chefia imediata informar às(aos) gestoras(es) do ativo a movimentação e o desligamento de qualquer usuária(o) alocada(o) em sua unidade, dadas as implicações na manutenção de direitos de acesso aos ativos de informação.

§ 1º A retirada da(o) usuária(o) dos acessos citados no *caput* somente se dará após a mudança de lotação ou desligamento efetuado no sistema de gestão de recursos humanos.

§ 2º Periodicamente, a unidade de defesa cibernética Tecnologia da Informação fará o bloqueio automático das credenciais de acesso das(o) usuárias(os) que não realizaram o acesso por mais de 45 (quarenta e cinco) dias, incluídos as(os) servidoras(es) aposentadas(os), cedidas(os) e licenciadas(os).

§ 3º Caso a inatividade do acesso de que trata o parágrafo anterior tenha ocorrido em razão de afastamento, ou outro motivo legítimo, a(o) usuária(o) poderá solicitar o desbloqueio da conta através dos canais de atendimento da Central de Serviços de TI (Service Desk).

Art. 29. Identidades digitais atribuídas a sistemas de informação em homologação ou produção e acesso ao banco de dados do Tribunal estão sujeitas às mesmas diretrizes e boas práticas de gestão de identidades lógicas definidas nesta norma, incluindo:

I - a Secretaria de Tecnologia da Informação deverá manter um inventário de contas de sistemas e serviços, devendo conter, no mínimo, a(o) gestora(or) proprietária(o), o sistema de informação ao qual a credencial está vinculada, data de revisão e propósito;

II - para cada sistema ou serviço deve ser feito o cadastro de login único por meio de serviço de diretório centralizado, recebendo identificação compatível com o sistema ou finalidade a qual estará associada;

III - deve ser adotado requisitos de tamanho, critérios de complexidade e período de expiração de senhas compatíveis com esta norma;

IV - devem ser usados mecanismos seguros de criptografia para o armazenamento e trânsito de credenciais de sistemas;

V - deve ser realizado o registro e armazenamento de todos os eventos significativos sobre o uso e gestão dos acessos e tentativas de acesso para identificação de ataques; e

VI - deverá ser feita a revisão e análise periódica recorrente, no mínimo trimestralmente ou com mais frequência, para validar se todas as contas/credenciais ativas estão em uso ou autorizadas.

Art. 30. Os direitos de acesso das(os) usuárias(os) devem ser revistos em intervalos regulares, bem como após qualquer mudança de nível institucional que implique em realocação de pessoas, unidades ou papéis.

Art. 31. As atividades de gerenciamento de identidades, acesso e autenticação devem ser registradas e arquivadas.

Parágrafo único. Deverão ser emitidos, frequentemente, relatórios críticos com finalidade de identificar inconsistências nestas atividades, atentando-se às recomendações anteriores bem como para as seguintes:

I - identificação de forma periódica de usuárias(os) redundantes; e

II - identificação de solicitações de acesso sem segregação de funções.

Art. 32. Devem ser incluídas cláusulas nos contratos de prestadoras(es) de serviço elencando sanções nos casos de acesso não autorizado, ou mesmo tentativa, efetuado por pessoa ou agente, mediante ações diretas ou indiretas das(dos) suas(seus) colaboradoras(es).

Art. 33. Compete à(ao) Gestora(or) de ativo realizar a revisão de direitos de acesso ao ativo sob sua responsabilidade, podendo a Secretaria de Tecnologia da Informação automatizar o processo de retirada de acessos e alteração de perfil para usuárias(os), nos casos previstos nos arts. 29 e 30, conforme as regras estabelecidas formalmente.

Seção III

Da Política de Senhas

Art. 34. Os sistemas ou serviços de informação, considerados passíveis de controle de acesso pela(o) gestora(or) de ativo, devem ter seu acesso restrito e controlado através do uso de senhas, token ou mecanismo de autenticação similar.

§ 1º Serão concedidas senhas temporárias, mediante concordância e assinatura de termo de confidencialidade de toda senha, ou outro mecanismo de autenticação que estiver em sua posse.

§ 2º O acesso remoto à rede, o acesso administrativo e o acesso a aplicações expostas externamente se darão por autenticação multifatorial (MFA).

§ 3º A Secretaria de Tecnologia da Informação, em conjunto com a(o) gestora(or) do ativo de informação, podem implementar a autenticação de multifatores para determinados tipos de acesso, em função de sua criticidade.

§ 4º As senhas associadas às contas de acesso a ativos/serviços de informação ou recursos computacionais do TRE-MS são de uso pessoal e intransferível, devendo a(o) usuária(o) zelar por sua guarda e sigilo.

Art. 35. A senha de acesso da(o) usuária(o), tokens, e outros fatores de autenticação devem ser de uso pessoal e intransferível.

Art. 36. As senhas devem ser secretas e definidas considerando as seguintes recomendações:

I - utilizar números, letras, alternando-as entre maiúsculas, minúsculas e caracteres especiais, como $@#&%, com, no mínimo, 12 (doze) caracteres para contas com autenticação de multifatores e 16 (dezesseis) caracteres para contas que não usam MFA;

II - não utilizar frases ou palavras que possam ser facilmente adivinhadas por terceiros, baseadas nas informações relativas à(ao) própria(o) usuária(o), tais como nome de parentes, datas de aniversário e números de telefone;

III - não utilizar senhas formadas por sequência de caracteres triviais – tais como 123456 ou abcde – ou senhas simples que repitam a identificação da(o) usuária(o) como, por exemplo, usuário joao.silva e senha joao.silva, ou ainda caracteres idênticos repetidos;

IV - modificar a senha temporária no primeiro logon; e

V - não expor a senha em local visível para terceiros, como anotações em papéis, sob pena de responsabilização pelos acessos indevidos.

Parágrafo único. A política de senhas associada aos Sistemas Eleitorais será definida pelo Tribunal Superior Eleitoral - TSE.

Art. 37. Não utilizar as mesmas credenciais (nome de usuário e/ou senha) para fins pessoais (em serviços externos ao ambiente de TI da Justiça Eleitoral) e profissionais.

Art. 38. A(O) usuária(o) deve evitar usar o recurso de salvar senhas no navegador web.

Art. 39. Sempre que houver comprovação de comprometimento de credencial, a equipe de defesa cibernética estará autorizada a efetuar o bloqueio temporário do login, com posterior

comunicação à(ao) titular para que realize imediata alteração da senha.

Parágrafo único. A(O) usuária(o) deve realizar alteração de sua senha de acesso em caso de suspeita de vazamento de dados, bem como comunicar a ocorrência à Central de Serviços de TI (Service Desk) da Secretaria de Tecnologia da Informação.

Art. 40. O sistema de gerenciamento de senha deve:

I - permitir que as(os) usuárias(os) selecionem e modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros;

II - deve prover orientações e recomendações relacionadas ao uso de senhas fortes;

III - forçar as mudanças de senha a intervalos regulares de, no máximo, 6 (seis) meses, ou intervalos menores, conforme política definida pelo Núcleo de Segurança da Informação;

IV - manter um registro das senhas anteriores utilizadas e bloquear a reutilização;

V - empregar criptografia no canal de comunicação utilizado para o tráfego de credenciais de acesso;

VI - criptografar ou embaralhar (hash) com salt as credenciais de autenticação armazenadas;

VII - não mostrar as senhas na tela quando forem digitadas;

VIII - garantir a modificação das senhas temporárias no primeiro acesso ao sistema ou serviço de informação;

XI - manter, para fins de auditoria, registro dos acessos, das operações e dos respectivos períodos;

X - desabilitar as contas que não possam ser associadas a uma(um) usuária(o) ou processo de negócio;

XI - monitorar tentativas de acesso a contas desativadas;

XII - monitorar as trocas de senhas de usuárias(os) privilegiadas(os); e

XIII - impor alterações de senha conforme necessidade do órgão, por exemplo, após um incidente de segurança.

Art. 41. A senha temporária, para primeiro acesso ou no caso de a(o) usuária(o) esquecer a sua senha, deverá ser emitida através de procedimento instruído pela unidade técnica de Segurança da Informação e aprovado pela Comissão de Segurança da Informação, no qual deverá informar dados pessoais para confirmação de identidade.

Parágrafo único. Fica vedada a emissão de senha para ciência de terceiros, ainda que chefes imediatos ou superiores do usuário, bem como o seu envio através de texto claro ou correio de terceiro.

Art. 42. A gestão das senhas utilizadas em certificados digitais (PIN/PUK e revogação) será de responsabilidade exclusiva de seus titulares.

Seção IV

Do Acesso Privilegiado

Art. 43. O acesso privilegiado aos sistemas e ativos de informação somente será concedido às(aos) usuárias(os) que tenham como atribuição funcional o dever de administrá-los.

§ 1º A política que trata o *caput* deve ser aplicada apenas a indivíduos com a competência necessária para realizar atividades que exijam acesso privilegiado e com base no requisito mínimo para seus papéis funcionais.

§ 2º O acesso privilegiado deve ser concedido à(ao) usuária(o) por meio de credenciais de acesso exclusivas para este fim, distintas das credenciais de acesso concedidas a esta(e) usuária(o) para a realização de suas atividades normais de negócio.

§ 3º A unidade de segurança e defesa cibernética deverá estabelecer procedimento de autorização e concessão de acesso privilegiado, devendo manter arquivo de registro contendo informações

sobre este pedido para posterior auditoria.

§ 4º O gestor do ativo de informação deve definir prazos de expiração para as credenciais de acesso privilegiado, ou seja, requisitos para o término dos direitos, após os quais deve ser reavaliado o atendimento aos critérios para a atribuição de acesso privilegiado ao detentor das credenciais expiradas.

§ 5º A solicitação de acesso privilegiado para qualquer unidade que não seja gestora do ativo deverá ser encaminhada através de processo administrativo à(ao) Presidente da Comissão de Segurança da Informação, para análise e parecer sobre a autorização.

§ 6º Os requisitos de autenticação para direitos de acesso privilegiados devem ser maiores do que os requisitos usados nos acessos normais, tais como, comprimento e complexidade de senha, uso de recurso MFA ou até mesmo equipamentos específicos.

§ 7º A unidade de Segurança da Informação e Defesa Cibernética deve considerar conceder o acesso privilegiado temporário apenas pelo período necessário para implementar alterações ou atividades aprovadas (por exemplo, para atividades críticas ou mudanças), em vez de conceder permanentemente direitos de acesso privilegiado. Este procedimento pode ser automatizado por soluções ou tecnologias de gerenciamento de acesso privilegiado.

§ 8º A quantidade de usuárias(os) de acesso privilegiado ao serviço de diretório deve ser limitada ou reduzida a um número mínimo necessário para desempenho das atividades de manutenção do ambiente.

Art. 44. As competências das(os) usuárias(os) com acesso privilegiado aos sistemas e ativos de informação deverão ser avaliadas em intervalos não superiores a um mês, para que estejam alinhadas às diretrizes desta norma, obedecendo as regras de segregação de funções.

Art. 45. O acesso privilegiado aos sistemas e ativos de informação através do uso de ID de usuária(o) administradora(or) genérica(o) deve ser evitado, se o sistema assim permitir e, quando não houver esta possibilidade, deve ser concedido mediante procedimentos de troca periódica de senha e auditoria dos acessos, criados pela(o) gestora(or) do ativo.

§ 1º Após a saída ou mudança de lotação de usuária(o) com conhecimento de senha de usuária(o) administradora(or) genérica(o), esta deve ser imediatamente modificada.

§ 2 º A conta de administradora(or) genérica(o) deve ser renomeada e ter sua função apagada, para que não possa ser facilmente identificada.

§ 3 º A conta de administradora(or) genérica(o) não deve ser usada para acesso à internet, iniciar serviços de rede e acessar arquivos externos.

§ 4 º A unidade de segurança e defesa cibernética deverá habilitar recurso de cofre de senhas e autenticação multifator MFA para todos os acessos à conta de administradora(or) genérica(o), incluindo os acessos privilegiados a banco de dados, plataformas de virtualização e ativos de segurança da informação.

Art 46. A unidade de segurança e defesa cibernética deverá habilitar recurso de proteção para impedir o logon de contas de administradora(or) genérica(o) em estações de trabalho.

Art. 47. Os direitos de acesso das(os) usuárias(os) privilegiadas(os) devem ser revistos em intervalos regulares, bem como após qualquer mudança de nível institucional que implique em realocação de pessoas, unidades ou papéis, considerando ainda a consistência entre os direitos de acesso e as necessidades e requisitos de segurança.

Art. 48. Evitar (ou remover) a integração do sistema de diretórios com soluções de backup, sistemas de virtualização, banco de dados e outras que possuam a possibilidade de integração com finalidade de administração, objetivando mitigar a propagação de ataques cibernéticos.

Seção V

Dos Procedimentos Seguros de Entrada no Sistema

Art. 49. O procedimento adequado de entrada no sistema (login) deve atender às seguintes recomendações:

I - não fornecer mensagens de ajuda ou informações do sistema durante o procedimento de entrada que possam auxiliar uma(um) usuária(o) não autorizada(o);

II - validar informações de entrada no sistema somente após todos os dados estarem completamente preenchidos;

III - no caso de erro, não indicar qual parte do dado de entrada está correta ou incorreta;

IV - bloquear o acesso da(o) usuária(o) ao sistema após, no máximo, 10 (dez) tentativas de entrada no sistema;

V - registrar tentativas de acesso ao sistema, sem sucesso e bem sucedidas;

VI - por ocasião da entrada no sistema, mostrar as seguintes informações:

a) data e hora da última entrada no sistema ou equipamento, com sucesso; e

b) detalhes de qualquer tentativa sem sucesso de entrada no sistema desde o último acesso com sucesso;

VII - encerrar sessões inativas após um período definido de inatividade de, no máximo, 10 (dez) minutos; e

VIII - em caso de uso externo, deve-se restringir o tempo de conexão para reduzir a oportunidade de acesso não autorizado.

Seção VI

Do Acesso dos Equipamentos à Rede e aos Serviços de Rede

Art. 50. As regras de controle de acesso deverão ser baseadas na premissa de que “tudo é proibido, a menos que expressamente permitido”, em lugar da regra “tudo é permitido, a menos que expressamente proibido”.

Art. 51. O acesso de novo equipamento à rede do Tribunal é regulamentado pelo procedimento de autorização específico e deverá ser executado através da abertura de chamado de requisição de serviço à Central de Serviços de TI (Service Desk);

Art. 52. São consideradas redes do TRE-MS para efeito de controle: a rede cabeada da sede e seus anexos, a rede cabeada dos Fóruns e Cartórios Eleitorais; todas as redes wifi em suas dependências e por ele provida; o acesso VPN; o perímetro para a internet.

Art. 53. É vedada a inclusão de equipamentos pessoais ou de terceiros em qualquer uma das redes internas do TRE, sem autorização da Secretaria de Tecnologia da Informação.

Art. 54. A inclusão de equipamentos de terceiros na rede será efetuada em subrede segura, distinta das demais e por período definido.

Art. 55. Os acessos à rede devem ser registrados, arquivados por um período mínimo de 6 (seis) meses, monitorados e frequentemente deve ser emitido relatório crítico com finalidade de identificar acessos indevidos.

Art. 56. Os serviços de rede que não estejam em uso devem ser removidos e não apenas desabilitados.

Art. 57. A STI deverá efetuar o bloqueio do uso de ferramentas e acesso remoto como o TeamViewer, Anydesk, Logmein, etc. e, caso haja necessidade de uso de ferramenta de acesso para suporte remoto, recomenda-se utilizar uma ferramenta corporativa com duplo fator de autenticação habilitado.

Capítulo VII

DA GESTÃO DE PROVEDORES DE SERVIÇOS

Art. 58. A política de segurança da informação deve estabelecer boas práticas de gestão de provedores de serviços, associada a empresas que mantêm, tratam ou compartilham dados sensíveis, ou são responsáveis por plataformas ou processos de TI críticos para o Tribunal, visando garantir que esses provedores estejam protegendo essas plataformas e dados de forma adequada.

Parágrafo único. A gestão de provedores de serviços deve abordar o inventário, classificação, avaliação, monitoramento e descomissionamento de provedores de serviços, atendendo as seguintes diretrizes:

I - estabelecer e manter um inventário de provedores de serviço, devendo o inventário:

a) listar todos os provedores de serviços, incluindo a razão social, o contato corporativo para cada provedor de serviços, a natureza do serviço, o número e a vigência do contrato, o objeto contratado, lista de colaboradores, dentre outras informações relevantes; e

b) ser revisado e atualizado anualmente ou quando ocorrerem mudanças significativas que possam impactar esta medida de segurança.

II - os provedores de serviço devem ser classificados considerando características como sensibilidade de dados tratados (quando houver), volume de dados, requisitos de disponibilidade, regulamentos aplicáveis e risco(s) inerente(s). A classificação dos provedores de serviço deve ser revisada e atualizada anualmente ou quando ocorrerem mudanças significativas que possam impactar esta medida de segurança;

III - devem ser incluídas cláusulas nos contratos com provedores de serviços que incluam requisitos de segurança consistentes com a política de segurança da informação da Justiça Eleitoral, como: notificação e resposta de incidente de segurança e/ou de violação de dados, requisitos de criptografia de dados e compromissos de descarte de dados;

IV - considerando a Segurança da Informação e proteção de dados, devem ser previstas cláusulas nos contratos que incluam a assinatura de Termo de Compromisso de Manutenção de Sigilo e Confidencialidade, assim como as(os) respectivas(os) funcionárias(os) alocadas(os) ao contrato deverão assinar Termo de Ciência/Sigilo, caso haja a necessidade de acessos à informações críticas ou tratamento de dados pessoais ou sensíveis;

V - devem ser incluídas cláusulas nos contratos prevendo o monitoramento de requisitos, o qual deve ser revisado e atualizado anualmente ou quando ocorrerem mudanças significativas que possam impactar esta medida de segurança, visando aferir a execução do contrato em conformidade à lista de verificação dos itens de segurança da informação que devem ser atendidos pelo provedor de serviço, considerando as boas práticas da política de segurança da informação da Justiça Eleitoral; e

VI - a gestão de provedores de serviços deve adotar procedimentos para descomissionar os prestadores de serviços com segurança, a exemplo de desativação de contas de usuário e serviço, encerramento de fluxos de dados e descarte seguro de dados corporativos em sistemas de provedores de serviços, após a revogação dos direitos ou o encerramento das atividades, contratos ou acordos, ou ajustados após qualquer mudança de atribuições.

Capítulo VIII

DO ACESSO REMOTO AOS SERVIÇOS E À REDE CORPORATIVA DO TRIBUNAL

Art. 59. No caso de imperiosa necessidade para desempenho do trabalho, as(os) usuárias(os) poderão solicitar acesso remoto a aplicações, serviços e infraestrutura de rede, mediante solicitação justificada da chefia imediata à Central de Serviços de TI (Service Desk).

Parágrafo único. Conceitua-se por acesso remoto o acesso disponibilizado pela Secretaria de Tecnologia da Informação via Portal de Aplicações para acesso externo aos aplicativos disponíveis na intranet do Tribunal, e infraestrutura VPN (Virtual Private Network ou Rede Privada Virtual), conforme regras específicas e características técnicas de cada serviço.

Art. 60. As concessões de acesso VPN (Virtual Private Network ou Rede Privada Virtual) estão restritas apenas às necessidades de teletrabalho formalmente autorizado pela administração, acesso para atendimento itinerante da Justiça Eleitoral e Postos de Atendimento Eleitoral (PAE).

§ 1º Todas as solicitações de acesso remoto associadas à infraestrutura de VPN deverão ser solicitadas e autorizadas mediante processo SEI, onde as(os) usuárias(os) devem assinar eletronicamente o Termo de Responsabilidade Acesso Rede Privada Virtual (Anexo II), quando da cessão do acesso VPN, anuindo com as condições desta Resolução e demais normas de Segurança de Informação, Privacidade e Proteção de Dados Pessoais correlatas.

§ 2º Para o atendimento da solicitação, a(o) usuária(o) deverá informar todos os sistemas que forem necessários ao acesso remoto para o desenvolvimento do trabalho.

§ 3º A Secretaria de Tecnologia da Informação poderá aprovar ou vetar as solicitações que tratam o caput por questões de segurança ou falta de compatibilidade da solicitação com a finalidade do recurso.

Art. 61. Para fins de otimizar o monitoramento, elevar o grau de segurança dos sistemas de TIC e mitigar riscos de ataques cibernéticos, ocorrerá bloqueio automático da infraestrutura de acesso remoto VPN diariamente, das 22:00h até ás 05:00h do dia seguinte, de segunda-feira a sexta-feira, ficando indisponível integralmente aos sábados, domingos e feriados.

Parágrafo único. Qualquer alteração excepcional nos dias e horários definidos no caput deverá ser solicitada à Comissão de Segurança da Informação.

Art. 62. Deve ser verificada a viabilidade técnica de restrição do acesso internacional aos serviços de acesso remoto e aplicações.

Art. 63. É facultado à STI exigir autenticação de dois fatores para acesso remoto aos serviços e à rede corporativa do Tribunal.

Art. 64. As permissões concedidas aos usuários para acesso remoto deverão atender ao princípio do menor privilégio, de forma que seja disponibilizada para o usuário apenas os serviços que forem estritamente necessários para o desenvolvimento do trabalho do usuário.

Art. 65. O acesso remoto à rede do Tribunal não poderá ser realizado a partir de computadores de uso público e por meio de redes sem fio públicas.

Art. 66. Objetivando mitigar o risco de ataque cibernético, a Secretaria de Tecnologia da Informação, a seu critério exclusivo, poderá fornecer notebooks ou computadores às(aos) servidoras(es) para uso do acesso remoto, condicionado à viabilidade técnica e disponibilidade de recursos.

§ 1º Os equipamentos fornecidos pela Secretaria de Tecnologia da Informação para acesso remoto à rede corporativa somente devem ser utilizados para atividades da Justiça Eleitoral ou a elas diretamente correlatas.

§ 2º O extravio do equipamento ou certificado utilizados para acesso remoto deverá ser imediatamente comunicado à Secretaria de Tecnologia da Informação.

§ 3º Nos casos em que o acesso remoto seja autorizado a ser feito pelo equipamento pessoal da(o) servidora(or), a Secretaria de Tecnologia da Informação está desobrigada a prestar suporte técnico para problemas de hardware ou softwares do equipamento pessoal da(o) servidora(or).

Art. 67. O suporte técnico para o acesso remoto aos recursos de TI do Tribunal estará disponível durante o horário de expediente do Tribunal.

Art. 68. A(O) usuária(o), quando utilizar o acesso remoto, deverá permanecer conectada(o) apenas enquanto estiver efetivamente utilizando os serviços disponibilizados, devendo desconectar-se nas interrupções e no término do trabalho.

Art. 69. O acesso remoto poderá ser interrompido a qualquer momento, independente de comunicação à(ao) usuária(o), na hipótese de ser identificada situação de grave ameaça ou alto risco à integridade da rede interna e dos serviços disponíveis.

Art. 70. Fica vedada a utilização de outros aplicativos de acesso remoto sem o conhecimento e autorização expressa da Secretaria de Tecnologia da Informação.

Art. 71. Os acessos à rede devem ser registrados, arquivados por um período mínimo de 6 (seis) meses, monitorados e frequentemente devem ser emitidos relatórios críticos com finalidade de identificar acessos indevidos.

Capítulo IX

DO CONTROLE DE ACESSO AO CÓDIGO-FONTE DE PROGRAMAS

Art. 72. O código-fonte e itens associados (esquemas, especificações, planos de validação, etc) dos sistemas de informação desenvolvidos pelo Tribunal somente serão acessíveis pelas(os) usuárias(os) que tenham como atribuição funcional seu desenvolvimento, manutenção ou outra atividade para a qual o acesso seja imprescindível.

§ 1º As bibliotecas de código-fonte e itens associados devem ser armazenadas em ferramentas apropriadas para este fim, em ambientes segregados dos sistemas operacionais onde os respectivos sistemas de informação sejam executados.

§ 2º Os eventos de acesso às bibliotecas de código-fonte e itens associados devem ser registrados, permitindo sua auditoria.

§ 3º Os códigos-fonte que sejam publicados para entidades externas devem contar com controles adicionais que garantam sua integridade.

Capítulo X

DISPOSIÇÕES FINAIS

Art. 73. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação deste Tribunal.

Art. 74. Fica revogada a Resolução n.º 663/2019 - TRE/MS - de 16 de setembro de 2019 e demais disposições em contrário.

Art. 75. Esta norma complementar deve ser revisada a cada 12 (doze) meses pelo Gestor de Segurança da Informação e encaminhada para nova apreciação da Comissão de Segurança da Informação.

Art. 76. Esta política deve ser publicada no portal de intranet do Tribunal pela Comissão de Segurança da Informação.

Art. 77. O descumprimento desta norma será objeto de apuração pela unidade competente do Tribunal, com a consequente aplicação das penalidades cabíveis a cada caso.

Art. 78. Esta Resolução entra em vigor na data de sua publicação e sua implementação inicia-se imediatamente.

ANEXO I [MODELO]

TERMO DE RESPONSABILIDADE DE ACESSO À REDE

1. Pelo presente termo, eu _____, CPF_____, e lotada(o) na(o) _____ do Tribunal Regional Eleitoral de Mato Grosso do Sul / TRE-MS, declaro, sob pena das sanções cabíveis, nos termos da legislação vigente, ter recebido autorização superior para uso de credenciais de acesso à Rede do TRE-MS, objetivando o desempenho das minhas funções profissionais, com privilégios adequados e suficientes ao exercício das atividades que aqui executo, sendo responsável pelo seu uso e guarda.

2. Declaro ter conhecimento da Política de Segurança da Informação do Tribunal Regional Eleitoral de Mato Grosso do Sul e a Política Geral de Privacidade e Proteção de Dados Pessoais do Tribunal Regional Eleitoral de Mato Grosso do Sul, disponíveis para consulta no sítio da internet do Tribunal e concordo em aceitar suas regras, assim como às diretrizes definidas na Resolução de Controle de Acesso Físico e Lógico.

3. Declaro estar ciente de que minhas ações, utilizando credenciais de acesso à Rede do TRE-MS, serão passíveis de auditoria e monitoramento de acordo com a Política de Segurança da Informação do TRE-MS e de que qualquer alteração feita sob minha identificação, advinda de minha autenticação e autorização, é de minha responsabilidade.

4. Declaro estar ciente da necessidade de manutenção da segurança e confidencialidade de minha senha de acesso à Rede do Tribunal, alterando a mesma sempre que existir qualquer indício de possível comprometimento, em intervalos regulares de tempo ou com base no número de acessos, a critério da Secretaria de Tecnologia da Informação.

5. Declaro, ainda, estar plenamente esclarecida(o) e consciente que:

I - O acesso à informação não me garante direito sobre ela, nem me confere autoridade para liberar acesso a outras pessoas.

II - Constitui descumprimento de normas legais, regulamentares e quebra de sigilo funcional divulgar dados obtidos dos sistemas aos quais tenho acesso para outros servidores não envolvidos nos trabalhos executados.

III - Devo cumprir e fazer cumprir os dispositivos da Política de Segurança da Informação e das Normas Complementares de Segurança estabelecidas, bem como deste Termo de

Responsabilidade.

IV - Ressalvadas as hipóteses de requisições legalmente autorizadas, constitui infração funcional e penal a revelação de segredo do qual me apropriei em razão do cargo, sendo crime contra a administração pública a divulgação a quem não seja agente público da Justiça Eleitoral, das informações do(s) sistema(s) a que tenho acesso, estando sujeito às penalidades previstas em lei.

V - Sem prejuízo da responsabilidade penal e civil, e de outras sanções disciplinares, constitui falta de zelo e dedicação às atribuições do cargo e descumprimento de normas legais e regulamentares, não proceder com cuidado na guarda e utilização de senha ou emprestá-la a outro agente público, ainda que habilitado.

VI - Constitui infração funcional e penal inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos dos sistemas ou bancos de dados da Administração Pública, com o fim de obter vantagem indevida para si ou para outrem ou para causar dano, ficando o infrator sujeito às punições previstas no Código Penal Brasileiro, conforme responsabilização por crime contra a Administração Pública, tipificado no art. 313-A.

VII - Constitui infração funcional e penal modificar ou alterar o sistema de informações ou programa de informática sem autorização ou sem solicitação de autoridade competente; ficando o infrator sujeito às punições previstas no Código Penal Brasileiro, conforme responsabilização por crime contra a Administração Pública, tipificado no art. 313-B.

VIII - Constitui obrigação funcional a proteção aos dados pessoais, que tenha acesso, em razão do trabalho desenvolvido, seja da área administrativa ou de processos eleitorais, sendo proibido o repasse das informações, sob pena de incorrer nas sanções previstas da Lei Geral de Proteção de Dados Pessoais (Lei n.º 13709/2018).

6. Declaro, nesta data, ter ciência e estar de acordo com os procedimentos acima descritos, comprometendo-me a respeitá-los e cumpri-los plena e integralmente.

<Nome do Município>-MS, _____ de _____ de _____.

Nome e unidade organizacional

[Servidora(or) pública(o) / Colaboradora(or) / Estagiária(o)]

Nome e unidade organizacional

[titular da unidade, gestora(or) de contrato ou sistema]

ANEXO II [MODELO]

TERMO DE RESPONSABILIDADE ACESSO REDE PRIVADA VIRTUAL (VPN)

1. Pelo presente termo, eu _____, CPF_____, e lotada na(o) _____ do Tribunal Regional Eleitoral de Mato Grosso do Sul / TRE-MS, declaro, sob pena das sanções cabíveis, nos termos da legislação vigente, ter recebido autorização superior para obter credenciais de acesso VPN, para uso e desempenho das minhas funções profissionais, com privilégios adequados e suficientes ao exercício das atividades que aqui executo, sendo responsável pelo seu uso e guarda.

2. Declaro ter conhecimento da Política de Segurança da Informação do Tribunal Regional Eleitoral de Mato Grosso do Sul e a Política Geral de Privacidade e Proteção de Dados Pessoais do Tribunal Regional Eleitoral de Mato Grosso do Sul, disponíveis para consulta no sítio da internet e concordo em aceitar suas regras, assim como às diretrizes definidas na Norma Controle de Acesso Físico e Lógico.

3. Declaro que farei uso dos recursos da REDE PRIVADA VIRTUAL (VPN) do TRE-MS, estando ciente de que minhas ações, utilizando credenciais de acesso à Rede do TRE-MS, serão monitoradas de acordo com a Política de Segurança da Informação do TRE-MS e de que qualquer alteração feita sob minha identificação, advinda de minha autenticação e autorização, é de minha responsabilidade.

4. Declaro, ainda, estar plenamente esclarecida(o) e ciente:

I. Que o acesso aos recursos da VPN é concedido a cada usuário (a) de forma pessoal e intransferível.

II. Da necessidade de manter sigilo das informações de acesso ao ambiente de Rede do TRE-MS e do acesso remoto, seja ele por VPN ou Portal de Sistemas e Aplicativos.

III. Que não devo ceder, informar, emprestar, passar e/ ou o que o valha, a chave ou credencial de acesso da VPN para terceiros em hipótese alguma; sendo de sua total e exclusiva responsabilidade qualquer operação realizada por meio de suas credenciais de acesso remoto.

IV. Que devo comunicar imediatamente à Secretaria de Tecnologia da Informação (STI) qualquer irregularidade ou situações que coloquem em risco o acesso ao ambiente computacional do TRE-MS.

V. Da necessidade de tratar qualquer incidente de segurança que venha ser identificado com urgência e prioridade adequados, evitando toda e qualquer forma de postergação.

VI. Da vedação quanto a utilização dos recursos da VPN para fins não relacionados às atividades do Tribunal, devendo o acesso restringir-se à esfera laboral, observando-se sempre a conduta compatível com a moralidade administrativa.

VII. Que a não observância das diretrizes da Política de Segurança da Informação e normas complementares pode resultar na suspensão imediata do acesso aos recursos da VPN de forma temporária ou permanente, bem como responder, em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam por em risco ou comprometer a Rede do Tribunal que tenho acesso.

VIII. Dos perigos de responder mensagens não solicitadas, acessar links ou baixar arquivos e anexos de origem desconhecida, bem como, conectar-se, ou manter-se conectado, a redes públicas durante o acesso a rede interna do Tribunal.

IX. Da necessidade de cuidar da proteção do computador e/ou notebook, que será(ão) utilizado(s) para acesso a rede interna do TRE-MS, por meio da instalação e atualização de antivírus e/ou outras soluções de segurança, bem como, de manter o Sistema Operacional (Windows e/ou Linux) atualizado.

5. Declaro, nesta data, ter ciência e estar de acordo com os procedimentos acima descritos, comprometendo-me a respeitá-los e cumpri-los plena e integralmente.

<Nome do Município>-MS, _____ de _____ de _____.

Nome e unidade organizacional

[Servidora(or) pública(o)/Colaboradora(or)/Estagiária(o)]

Nome e unidade organizacional

[titular da unidade, gestora(or) de contrato ou sistema]

Sala de Sessões do Tribunal Regional Eleitoral.

Em Campo Grande, MS, aos 20 de maio de 2025.

Desembargador CARLOS EDUARDO CONTAR

Presidente

Desembargador SÉRGIO FERNANDES MARTINS

Vice-Presidente e Corregedor Regional Eleitoral

Dr. VITOR LUÍS DE OLIVEIRA GUIBO

Juiz de Direito

Dr. CARLOS ALBERTO ALMEIDA DE OLIVEIRA FILHO

Advogado

Dr. FERNANDO NARDON NIELSEN

Juiz Federal

Dr. ALEXANDRE ANTUNES DA SILVA

Juiz de Direito

Dr. MÁRCIO DE ÁVILA MARTINS FILHO

Advogado

Dr. LUIZ GUSTAVO MANTOVANI

Procurador Regional Eleitoral

Documento assinado eletronicamente por **Luiz Gustavo Mantovani**, **Usuário Externo**, em 20/05/2025, às 19:38, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **SÉRGIO FERNANDES MARTINS**, **Corregedor Regional Eleitoral**, em 21/05/2025, às 10:37, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **CARLOS ALBERTO ALMEIDA DE OLIVEIRA FILHO**, **Juiz Membro**, em 21/05/2025, às 17:09, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **VITOR LUIS DE OLIVEIRA GUIBO**, **Juiz Membro**, em 22/05/2025, às 11:04, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ALEXANDRE ANTUNES DA SILVA**, **Juiz Membro**, em 22/05/2025, às 14:58, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-ms.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1860141** e o código CRC **36053232**.

Certifico e dou fé que a Resolução nº 861, de 20.5.2025, foi publicada no DJe nº 105 de 27.5.2025, à(s) fl(s). 03/19.

(Matrícula 05040458)