Tribunal Regional Eleitoral de Mato Grosso do Sul

RESOLUÇÃO Nº 663

Dispõe sobre a instituição da Política de Controle de Acesso Físico e Lógico relativamente à Segurança das Informações deste Tribunal Regional, e dá outras providências.

O egrégio **TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO DO SUL**, no uso de suas atribuições que lhe confere o art. 21, inciso XXX, de seu Regimento Interno – Resolução nº 170/2007, bem como em consonância com o que ficou decidido em sessão plenária realizada nesta data a par do que consta no Processo Administrativo SEI nº 007400-21.2019.6.12.8000,

Considerando as orientações de controle de segurança da informação dispostas na norma ISO NBR/IEC 27002:2013, às quais esta Política de Controle de Acesso Físico e Lógico encontra-se efetivamente alinhada;

Considerando a NC 07/IN01/DSIC/GSIPR, de 15.7.2014, que estabelece diretrizes para implantação de controles de acesso relativos à segurança da informação e comunicações na Administração Pública Federal;

Considerando as recomendações do Acórdão TCU nº 1.603/2008, item 9.1.3, sobre a importância dos controles de acesso;

R E S O L V E:

Art. 1º Instituir a Política de Controle de Acesso Físico e Lógico relativamente à Segurança da Informação, integrante da Política de Segurança da Informação deste Tribunal Regional.

CAPÍTULO I
DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para os efeitos desta resolução e de suas regulamentações, aplicam-se as seguintes definições:

I – Acesso físico: é ato de ingressar e transitar fisicamente nas edificações e instalações da instituição.

II – Acesso lógico: é o acesso aos sistemas e ativos de informação.

III – Acesso privilegiado: é o acesso aos sistemas e ativos de informação com amplos poderes.

IV – Ativos de informação: patrimônio composto por todos os dados e informações gerados, adquiridos, utilizados ou armazenados pela Justiça Eleitoral.

V – Ativo de processamento: patrimônio composto por todos os elementos de hardware, software e infraestrutura de comunicação necessários à execução das atividades precípuas da Justiça Eleitoral.

VI – Autenticação de multifatores: utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema, tais como cartão por aproximação, PIN (*personal identification number*) e biometria.

VII – Autenticidade: propriedade que garante que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

VIII – Biometria: é a verificação da identidade de um indivíduo por meio de uma característica física ou comportamental única, através de métodos automatizados.

IX – Bloqueio de acesso: processo que tem por finalidade suspender o acesso.

X – Confidencialidade: propriedade da informação que garante que ela não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem a devida autorização.

XI – Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

XII – Disponibilidade: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada.

XIII – Fatores de autenticação: mecanismo utilizado para a concessão de acesso, como senhas, biometria, etc.

XIV – Gestor de ativo de informação: proprietário ou custodiante de ativo de informação, responsável por definir perfis de acesso e por aprovar ou reprovar solicitações de autorização de acesso aos ativos sob sua responsabilidade.

XV – Integridade: propriedade que garante que a informação mantém todas as características originais estabelecidas pelo proprietário.

XVI – Irretratabilidade (ou não repúdio): garantia de que a pessoa se responsabilize por ter assinado ou criado a informação

XVII – Necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação.

XVIII – Necessidade de uso: permissão para acessar os ativos de processamento da informação que o usuário necessita para desempenhar a sua tarefa.

XIX – Perfil de acesso: conjunto de permissões de acesso a ativo de informação específico, que pode ser atribuído a usuário ou grupo de usuários com necessidade de conhecer em comum.

XX – Perímetro de segurança física: fronteiras externas, normalmente os limites de uma propriedade; é a primeira linha de defesa contra invasões; pode ser composta por muros, cercas, alarmes, iluminação, CFTV e vigilância patrimonial.

XXI – Prestador de serviço: pessoa envolvida com desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderá receber autorização de acesso.

XXII – Usuário: pessoa que obteve autorização para acesso a ativos de informação.

CAPÍTULO II
DOS PRINCÍPIOS

Art. 3º A política de que trata esta resolução tem como princípio norteador a garantia da integridade, autenticidade, confidencialidade, disponibilidade e irretratabilidade dos ativos de informação e de processamento.

CAPÍTULO III
DO ESCOPO

Art. 4º O objetivo desta Política é estabelecer diretrizes para implantação de controles de acesso físico e lógico, visando à preservação dos ativos de informação sob a responsabilidade deste Tribunal Regional, respeitando os princípios norteadores.

Art. 5º Esta Política se aplica a todos os magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço, colaboradores e usuários externos que utilizam os ativos de informação e de processamento da Justiça Eleitoral.

Parágrafo único. Todos são corresponsáveis pela segurança da informação, devendo, para tanto, conhecer e seguir esta Política.

CAPÍTULO IV
DO CONTROLE DO ACESSO FÍSICO

Seção I
Do perímetro de segurança

Art. 6º A Comissão de Segurança da Informação deverá definir o perímetro de segurança física tanto das instalações dos ativos de informação e de processamento (*Datacenter*), como das demais áreas que contenham informações críticas ou sensíveis.

Parágrafo único. O controle de acesso físico aos prédios da Justiça Eleitoral deverá ser sugerido pela Comissão de Segurança da Informação, avaliado e, sendo possível de implantação, aprovado pela Diretoria-Geral da Secretaria e implantado pela unidade de segurança deste Tribunal Regional.

Art. 7º Para as instalações do *Datacenter*, este Tribunal Regional deverá atender às seguintes diretrizes:

I – espaço físico com paredes sólidas, sem janelas, brechas ou pontos onde possam ocorrer invasões;

II – espaço físico com portas robustas e com mecanismos de autenticação de multifatores, restrito apenas ao pessoal autorizado;

III – barreiras físicas, quando necessário e aplicável;

IV – que os acessos sejam registrados com data e hora da entrada e da saída e, no caso dos visitantes e prestadores de serviços externos, sejam supervisionados os acessos;

V – que seja mantida e monitorada de forma segura a trilha de auditoria eletrônica do registro de todos os acessos;

VI – que possua sistema para detecção de intrusos;

VII – que as instalações sejam projetadas para minimizar o risco de ameaças físicas potenciais e ambientais, como furto, incêndio, inundação, terremoto, explosão, manifestações civis e possíveis acidentes;

VIII – que possua proteção contra raios e todas as linhas de entrada de força e de comunicações tenham filtros de proteção contra raios;

IX – que possua no mínimo duas entradas de alimentação de energia elétrica e telecomunicações, com rotas físicas diferentes;

X – que possua iluminação e comunicação de emergência;

XI – que não permita o uso de máquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, como câmeras em dispositivos móveis, salvo se autorizado;

XII – que possua sistema de controle de temperatura e umidade com recurso de emissão de alertas, e

XIII – que possua sistema de vídeo-monitoramento interno e do perímetro.

Art. 8º As diretrizes para proteção das demais áreas que contenham informações críticas ou sensíveis que não estejam armazenadas no *Datacenter* deverão ser estabelecidas pela Comissão de Segurança da Informação, observados os requisitos de segurança dos ativos existentes no interior do perímetro, o resultado da avaliação de riscos e as legislações vigentes.

Seção II
Dos ativos de Tecnologia da Informação

Art. 9º Para evitar perdas, danos, furtos, ou comprometimento de ativos e interrupção das operações da organização, este Tribunal Regional deverá seguir as seguintes diretrizes:

I – implantar uma área de recepção ou outro meio para controlar o acesso físico ao edifício para evitar acesso não autorizado aos ativos;

II – proibir que os usuários comam ou bebam próximo aos ativos;

III – implantar proteção contra raios para todo o edifício;

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

V – implantar a gestão dos ativos neste Tribunal Regional;

VI – que a manutenção dos ativos de processamento seja realizada somente por pessoal de manutenção autorizado;

VII – manter registro de todas as falhas, suspeitas ou reais, e de todas as operações de manutenção preventiva e corretiva realizadas dos ativos;

VIII – eliminar as informações sensíveis dos ativos, no caso de manutenção externa, quando possível, ou analisar os riscos de sua exposição;

IX – inspecionar o equipamento, após a manutenção externa, para garantir que não foi alterado indevidamente e que está em bom funcionamento;

X – os ativos, fora das dependências deste Tribunal Regional, não podem ficar sem supervisão;

XI – observar as instruções do fabricante sobre a proteção dos equipamentos, tais como exposição a campos eletromagnéticos;

XII – adotar controles para a movimentação dos ativos fora das dependências do Tribunal, bem como a aplicação de todos os controles para a segurança das informações contidas no ativo, e

XIII – adotar controles para evitar a retirada de equipamentos deste Tribunal sem prévia autorização.

Seção III
Da segurança do cabeamento

Art. 10. O cabeamento de energia elétrica e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deverá ser protegido contra interceptação, interferência ou danos, conforme as seguintes diretrizes:

I – as linhas de energia elétrica e de telecomunicações que entram nas instalações onde se encontram os ativos de informação e de processamento deverão ser subterrâneas ou fiquem abaixo do piso sempre que possível ou, no caso de ser aérea, recebam uma proteção alternativa adequada, e

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

Seção IV
Da reutilização ou descarte seguro dos ativos de processamento ou equipamentos em prova de conceito

Art. 11. Todos os ativos de processamento que contenham dados armazenados devem ser examinados antes da reutilização ou descarte para assegurar que

todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança.

Parágrafo único. Os ativos de processamento que contenham informações confidenciais ou de direitos autorais, quando possível, deverão ser destruídos fisicamente ou as informações deverão ser destruídas, apagadas ou sobregravadas por meio de técnicas que as tornem irrecuperáveis.

Seção V
Dos ativos de Informação

Art. 12. Com o objetivo de evitar a exposição desnecessária e o comprometimento de informações sensíveis ou críticas, este Tribunal Regional deve estabelecer a política de mesa limpa e tela limpa, que busca reduzir o risco de acesso não autorizado, perda e dano da informação.

Parágrafo único. Para efeito do que trata o *caput*, serão adotadas as seguintes diretrizes:

I – papéis ou mídia removível com informações sensíveis ou críticas deverão ser guardadas em lugar seguro, tais como cofre, armário com chave ou outra mobília segura, quando não estiverem em uso, mesmo que seja uma ausência temporária;

II – bloquear o computador, quando sair de sua mesa de trabalho temporariamente e fazer *logoff* quando se ausentar por um período longo, para evitar acesso indevido por outras pessoas;

III – documentos que contém informações sensíveis ou críticas quando enviados para impressão sejam removidos imediatamente, e

IV – para o estabelecimento de informações sensíveis ou críticas, deve-se considerar a resolução de classificação da informação deste Tribunal Regional.

CAPÍTULO V
DO CONTROLE DO ACESSO LÓGICO

Seção I
Do gerenciamento de acesso

Art. 13. As operações de registro, alteração (mudança de lotação ou mudança de função) e cancelamento de usuários da rede local devem ser solicitadas a este Tribunal Regional, conforme a seguir discriminados:

I – à Secretaria de Tecnologia de Informação – STI, pelo sistema da central de serviços:

II – pela Secretaria de Gestão de Pessoas, para os magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo e estagiários;

III – pela fiscalização administrativa dos contratos, para os prestadores de serviços, e

IV – pela Diretoria-Geral, para os demais casos.

§ 1º Qualquer colaborador que possuir prazo determinado de permanência na Justiça Eleitoral deverá ter suas credenciais criadas com a data de expiração conforme estabelecido.

§ 2º A STI irá definir um perfil padrão para os usuários novos, que já contemple as aplicações que todos os usuários devem ter acesso (e-mail, mensagem instantânea, acesso à internet entre outros).

Art. 14. É de responsabilidade da chefia imediata da unidade de lotação do usuário solicitar permissão de acesso aos sistemas ou serviços de informação, bem como o perfil de acesso que o usuário deverá possuir para cada sistema ou serviço de informação, através do sistema da central de serviços.

§ 1º O perfil de acesso do usuário aos sistemas ou serviços de informação será concedido conforme a necessidade de uso e a necessidade de conhecer, com base nos requisitos para sua função, observando-se a política de classificação da informação deste Tribunal Regional.

§ 2º O Gestor de Ativo de Informação ou serviço será responsável pela definição dos perfis de acesso e pela autorização dos direitos de acesso.

§ 3º Os acessos privilegiados deverão ser analisados criticamente e, preferencialmente, não sejam concedidos para as contas de operação do negócio e sim criação de contas temporárias e com prazo determinado para expiração.

Art. 15. Os usuários deverão possuir identificação única e exclusiva para permitir relacioná-la às suas ações.

Parágrafo único. É vedado aos usuários utilizarem sua identificação (usuário e senha) fornecida por este Tribunal Regional para cadastro em serviços externos não homologados ou autorizados.

Art. 16. Compete à chefia imediata informar, antecipadamente, aos responsáveis estabelecidos no art. 13 desta resolução, a movimentação ou o desligamento de qualquer usuário alocado sob sua responsabilidade, para que os direitos de acesso sejam alterados, ajustados ou cancelados imediatamente a movimentação ou desligamento.

Art. 17. Os direitos de acesso dos usuários deverão ser revistos em intervalos regulares e depois de qualquer mudança de função, alteração de lotação ou desligamento.

Parágrafo único. Compete ao Gestor de Ativo de Informação realizar a revisão de direitos de acesso ao ativo sob sua responsabilidade, bem como revisar os direitos de acesso dos usuários ao ativo.

Seção II
Da política de senhas

Art. 18. Os sistemas ou serviços de informação, considerados passíveis de controle de acesso pelo Gestor de Ativo, devem ter seu acesso restrito e controlado através do uso de senha, *token* ou mecanismo de autenticação similar.

Art. 19. A senha de acesso do usuário deverá ser secreta, de uso pessoal e intransferível, considerando as seguintes recomendações:

I – usar números, letras, alternando-as entre maiúsculas e minúsculas, e caracteres especiais, como $@#&%, com, no mínimo, oito caracteres;

II – não usar frases ou palavras que possam ser facilmente adivinhadas por terceiros, baseadas nas informações relativas ao próprio usuário, 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 do usuário como, por exemplo, usuário joao.silva e senha joao.silva, e

IV – não usar a senha de uso pessoal para senhas de uso profissional.

Art. 20. É proibido o compartilhamento de identificação de usuário e senha, bem como a exposição em local visível para terceiros, como anotações em papéis, sob pena de responsabilização pelos acessos indevidos.

Art. 21. Sempre que houver indicação de possível comprometimento da senha, deverá ser realizada a sua alteração.

Art. 22. O sistema de gerenciamento de senha dos ativos de informação e serviços deverá:

I – permitir que os usuários selecionem e modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros;

II – forçar as mudanças de senha a intervalos regulares, de no máximo seis meses, conforme necessidade;

III – manter um registro das senhas anteriores utilizadas e bloquear a reutilização;

IV – armazenar e transmitir as senhas de forma protegida;

V – não mostrar as senhas na tela quando forem digitadas;

VI – a senha temporária deve ser uma identificação do usuário (CPF ou título, por exemplo), e

VII – no primeiro acesso ao sistema ou serviço de informação, a senha temporária/inicial deverá ser alterada obrigatoriamente.

Seção III
Dos procedimentos seguros de entrada nos Sistemas

Art. 23. O procedimento adequado de entrada nos sistemas (*login)* deve atender às seguintes recomendações:

I – não fornecer mensagens de ajuda durante o procedimento de entrada que poderiam auxiliar um usuário não autorizado;

II – validar informações de entrada 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 do usuário após, no máximo, cinco tentativas de entrada nos sistemas;

V – registrar tentativas de acesso aos sistemas, tanto as sem sucesso como as bem-sucedidas;

VI – quando da entrada no sistema, mostrar as seguintes informações:

a) data e hora da última entrada com sucesso e o equipamento pelo qual fez o acesso;

b) detalhes de qualquer tentativa sem sucesso de entrada desde o último acesso com sucesso;

VII – não mostrar a senha que está sendo informada;

VIII – não transmitir senhas em texto claro pela rede, e

IX – encerrar sessões inativas após um período definido de inatividade, de no máximo dez minutos.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 24. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação deste Tribunal Regional.

Art. 25. A revisão desta Política de Controle de Acessos Físico e Lógico relativamente à Segurança da Informação ocorrerá sempre que se fizer necessário ou conveniente para este Tribunal Regional, não excedendo o período máximo de três anos.

Art. 26. Esta Política deverá ser publicada no portal da intranet deste Tribunal Regional pela respectiva Comissão de Segurança da Informação.

Art. 27. O descumprimento desta Política será objeto de apuração pela unidade competente deste Tribunal Regional e consequente aplicação das penalidades cabíveis a cada caso.

Art. 28. Esta resolução é de uso obrigatório.

Art. 29. Revogam-se as disposições em contrário.

Art. 30. Esta resolução entra em vigor nesta data.

Sala das Sessões do Tribunal Regional Eleitoral.

Em Campo Grande, MS, aos 16 de setembro de 2019.

Des. DIVONCIR SCHREINER MARAN
Presidente em substituição legal

Des. JULIZAR BARBOSA TRINDADE
Vice-Presidente e Corregedor Regional Eleitoral em substituição legal

Dr. ABRÃO RAZUK
Advogado

Dr. CLORISVALDO RODRIGUES DOS SANTOS
Juiz Federal

Dr. DANIEL CASTRO GOMES DA COSTA
Advogado

Dr. DJAILSON DE SOUZA
Juiz de Direito

Dr. JOSÉ HENRIQUE NEIVA DE CARVALHO E SILVA
Juiz de Direito

Dr. PEDRO PAULO GRUBITS GONÇALVES DE OLIVEIRA
Procurador Regional Eleitoral Substituto

PUBLICADO NO DJEMS Nº 2273
de 17 / 9 / 2019 fls. 20 a 26