TRIBUNAL REGIONAL ELEITORAL DE RONDÔNIA

Tribunal Regional Eleitoral - RO -

RESOLUÇÃO N. 41/2017

INSTRUÇÃO N. 0600032-42.2017.6.22.0000 - CLASSE 19 (SEI N. 0001522 - 10.2017.6.22.8000)

Relator: Des. Rowilson Teixeira
Interessado: Tribunal Regional Eleitoral de Rondônia

Dispõe sobre a instituição da Política de Controle de Acesso Físico e Lógico relativos à Segurança das Informações e Comunicações do Tribunal Regional Eleitoral de Rondônia.

O Tribunal Regional Eleitoral de Rondônia, no uso de suas atribuições, que lhe são conferidas pelo art. 13, inciso X, do Regimento Interno aprovado pela Resolução TRE/RO n. 36, de 10 de dezembro de 2009, e

considerando as orientações de controles de segurança da informação dispostas na norma ISO NBR/IEC 27002:2013;

considerando a NC 07/IN01/DSIC/GSIPR, de 15/07/2014, que estabelece diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações na Administração Pública Federal;

considerando as recomendações do Acórdão 1.603/2008-TCU, item 9.1.3, sobre a importância dos controles de acesso;

considerando a Resolução do TSE nº 23.501/2016, que instituiu a Política de Segurança da Informação no âmbito da Justiça Eleitoral, resolve:

Art. 1º Instituir a Política de Controle de Acesso Físico e Lógico relativos à Segurança das Informações e Comunicações no âmbito do Tribunal Regional Eleitoral de Rondônia;

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: são os meios de armazenamento, de transmissão e de processamento, bem como os sistemas de informação, as instalações e as pessoas que a elas têm acesso;

V - Ativos de processamento: patrimônio composto por todos os elementos de hardware, software e infraestrutura de comunicação necessários à execução das atividades precípuas do TRE-RO;

IV - Autenticação de multifatores: utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema;

VI - Biometria: é a verificação da identidade de um indivíduo por meio de uma característica física ou comportamental única, através de métodos automatizados;

VII - Bloqueio de acesso: processo que tem por finalidade suspender o acesso;

VIII - Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

IX - Fatores de autenticação: mecanismo utilizado para a concessão de acesso, como senhas, biometria etc;

X - 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;

XI - 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;

XII - Necessidade de uso: permissão para acessar os ativos da informação que o usuário necessita para desempenhar a sua tarefa;

XIII - 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;

XIV - Política de mesa limpa e tela limpa: práticas adotadas a assegurar que informações sensíveis, tanto em formato digital quanto físico, além de ativos de TI, como noteboooks, celulares, tablets, e outros, não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso, ou quando alguém deixa sua área de trabalho, seja por um curto período de tempo ou ao final do expediente de trabalho.

XV - 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;

XVI - Usuário: pessoa que obteve autorização para acesso a ativos de informação.

CAPÍTULO II

DOS PRINCÍPIOS

Art. 3º Esta Política tem como princípio norteador a garantia da integridade, confidencialidade e disponibilidade dos ativos de informação e dos ativos de processamento.

Art. 4º O acesso deverá ser concedido aos usuários deste Tribunal atendendo aos princípios norteadores da Política de Controle de Acesso Físico e Lógico relativos à Segurança das Informações e Comunicações e aos critérios da necessidade de conhecer e da necessidade de uso.

CAPÍTULO III

DO ESCOPO

Art. 5º O objetivo desta Política de Controle de Acesso Físico e Lógico relativos à Segurança das Informações e Comunicações é:

I - Estabelecer diretrizes para implementação de controles de acesso físico e lógico;

II - Preservar os ativos de informação; e,

III - Assegurar a confidencialidade, integridade e disponibilidade das informações sob a responsabilidade deste Tribunal.

Art. 6º Esta Política se aplica a todos os magistrados, membros do Ministério Público, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço e colaboradores, que fazem uso dos ativos de informação e de processamento no âmbito da Justiça Eleitoral de Rondônia.

Parágrafo único. Todos os magistrados, membros do Ministério Público, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço e colaboradores são corresponsáveis pela segurança da informação e comunicação, devendo, para tanto, conhecer e seguir esta Política.

CAPÍTULO IV

DO CONTROLE DO ACESSO FÍSICO

SEÇÃO I

DO PERÍMETRO DE SEGURANÇA

Art. 7º A Comissão de Segurança da Informação e Comunicação deverá definir o perímetro de segurança física para proteção tanto das instalações de processamento da informação como as áreas que contenham informações críticas ou sensíveis.

Art. 8º As instalações de processamento e armazenamento da informação, em especial o Data Center principal e o site backup, bem como as áreas que contenham informações criticas ou sensíveis, deverão atender às seguintes diretrizes:

I - Paredes fisicamente sólidas, sem brechas nem pontos onde poderia ocorrer uma invasão, portas externas adequadamente protegidas por mecanismos de controle contra acesso não autorizado e janelas com proteção externa;

II - Implantação de uma recepção para controlar o acesso físico ao edifício, com o registro do motivo e data e hora da entrada e saída do visitante ou prestador de serviço, previamente autorizado;

III - Mecanismos de autenticação de multifatores, para as instalações de processamento e armazenamento de informações, e que seja restrito apenas ao pessoal autorizado;

IV - Portas corta-fogo com sistema de alarme e que sejam monitoradas e testadas juntamente com as paredes, para estabelecer o nível de resistência exigido em normas regionais, nacionais e internacionais aceitáveis, bem como funcionem de acordo com os códigos locais de prevenção de incêndios e de falhas;

V - Sistemas para detecção de intrusos em todas as portas externas e janelas acessíveis;

VI - As instalações de processamento e armazenamento das informações sejam projetadas contra desastres naturais, tais como fogo, inundação, terremoto, explosão, manifestações civis; contra ataques maliciosos; e contra qualquer tipo de acidente;

VII - Os edifícios sejam dotados de proteção contra raios e todas as linhas de entrada de força e de comunicações tenham filtros de proteção contra raios;

VIII - Possua múltiplas alimentações de energia elétrica e telecomunicações, com rotas físicas diferentes;

IX - Instalação de iluminação e comunicação de emergência;

X - Sistema de controle de temperatura e umidade com recurso de emissão de alertas.

SEÇÃO II

DOS EQUIPAMENTOS DE PROCESSAMENTO E ARMAZENAMENTO

Art. 9º Para evitar perdas, danos, furtos, ou comprometimento de ativos e interrupção das operações da organização, o Tribunal deverá seguir as 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 - Proibir a ingestão de alimentos (comidas e bebidas) próximo às instalações de processamento e armazenamento da informação;

III - 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;

IV - 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 dado 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 de processamento da informação deverão ser subterrâneas ou fiquem abaixo do piso sempre que possível, ou recebam uma proteção alternativa adequada;

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

SEÇÃO IV

DA MANUTENÇÃO EXTERNA DOS EQUIPAMENTOS

Art. 11. A manutenção dos equipamentos de processamento de informações deverá seguir as seguintes diretrizes:

I - Realizar manutenção nos intervalos recomendados pelo fornecedor e de acordo com as suas especificações;

II - A manutenção e os consertos dos equipamentos sejam realizados somente por pessoal de manutenção autorizado;

III - Manter registro de todas as falhas, suspeitas ou reais, e de todas as operações de manutenção preventiva e corretiva realizadas;

IV - Eliminar as informações sensíveis do equipamento, quando possível, ou analisar os riscos de sua exposição;

V - Inspecionar o equipamento, após a manutenção, para garantir que não foi alterado indevidamente e que não está em mau funcionamento.

SEÇÃO V

DA REUTILIZAÇÃO OU DESCARTE SEGURO DOS EQUIPAMENTOS

Art. 12. Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes da reutilização, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança.

§1º Os equipamentos deverão ser inspecionados para verificar se a mídia está ou não armazenada, antes do descarte ou reutilização.

§2º As mídias que contenham informações confidenciais ou de direitos autorais sejam destruídas fisicamente, ou as informações sejam destruídas, apagadas ou sobregravadas por meio de técnicas que tornem as informações originais irrecuperáveis.

SEÇÃO VI

DA POLÍTICA DE MESA LIMPA E TELA LIMPA

Art. 13. A política de mesa limpa e tela limpa reduz o risco de acesso não autorizado, perda e dano da informação durante e fora do horário normal de trabalho.

§1º Política de mesa limpa para papéis e mídias de armazenamento removíveis deve considerar a classificação da informação, requisitos contratuais e legais e o risco correspondente.

§2º Política de tela limpa para computadores e terminais através de bloqueio por senha, token ou mecanismos de autenticação similar.

CAPÍTULO V

DO CONTROLE DE ACESSO LÓGICO

SEÇÃO I

DO GERENCIAMENTO DE ACESSO

Art. 14. Todo magistrado, servidor efetivo e requisitado, ocupante de cargo em comissão sem vínculo efetivo e estagiário que ingressar no TRE-RO, deve assinar um termo de responsabilidade para ter direito ao acesso às informações e aos recursos de Tecnologia da Informação. Este termo deve ser mantido pelo setor de Gestão de Pessoas e armazenado de modo seguro.

Parágrafo único. No caso de prestador de serviço ou fornecedor, que necessite acesso às informações ou recursos de Tecnologia da Informação, o fiscal do contrato ficará responsável por recolher a assinatura no termo de responsabilidade, a ser arquivado no respectivo processo de contratação.

Art. 15 Todos os acessos aos ativos de informação devem ser realizados através de solicitações formais de inclusão, suspensão, alteração de perfil e exclusão de usuários.

Parágrafo único. O controle de acesso lógico deve se basear na segregação de funções seguindo a premissa de que tudo é proibido a menos que expressamente permitido. As permissões devem considerar os princípios da "necessidade de conhecer" e "necessidade de uso", visando sempre o bom andamento das atividades jurisdicionais.

Art. 16. A criação de uma nova conta de acesso aos sistemas de informação, dar-se-á, por meio de solicitação formal à Central de Serviços de TI, contendo pelo menos:

I - nome completo, título de eleitor, lotação e matrícula do usuário;

II - a vigência do contrato no caso de estagiário ou prestador de serviços.

§ 1º A solicitação de criação de conta deverá ser feita:

I - Pela Secretaria de Gestão de Pessoas, após o devido cadastro no sistema de gestão, quando se tratar de magistrado, servidor efetivo e requisitado, ocupante de cargo em comissão sem vínculo efetivo e estagiário;

II - Pelo fiscal do contrato quando se tratar de terceirizados.

Parágrafo único. O processo de criação de conta de acesso aos sistemas de informação, com a definição das atividades, papéis, responsabilidades e demais atributos, quando instituído, poderá alterar o disposto neste artigo.

Art. 17. No ato da criação das contas de acesso citadas no artigo anterior, § 1º, inciso I, serão também criadas as respectivas contas de e-mail para uso exclusivamente institucional.

Parágrafo único. As regras de utilização do serviço de e-mail, bem como critérios de tamanho da caixa, arquivos anexos, dentre outros, serão objeto de norma complementar.

Art. 18. A Secretaria de Gestão de Pessoas deve informar à Central de Serviços de TI, as aposentadorias, vacâncias, exoneração ou redistribuição de magistrados e servidores, assim como o desligamento de magistrados e de estagiários, para as providências de eliminação das respectivas contas de usuários.

§ 1º. O desligamento de servidores terceirizados, deverá ser comunicado pelo gestor do contrato;

§ 2º. No caso de servidores cedidos a outros órgãos os direitos de acesso devem ser apenas suspensos.

Art. 19. A permissão ou revogação de acesso à informação deve ser autorizada pelo gestor de ativo de informação, mediante sistema específico ou registro de chamados na Central de Serviços de TI, fornecendo todos os dados necessários para a realização do cadastro ou mesmo alteração ou exclusão do acesso, se for o caso.

Art. 20. São responsabilidades do gestor de ativo de informação definir o perfil de acesso a ser atribuído a cada usuário, determinar as mudanças de perfil que se fizerem necessárias e solicitar o cancelamento do acesso quando este não for mais necessário.

§ 1º Qualquer autorização de acesso deverá estar de acordo com a Política de Classificação da Informação do Tribunal.

§ 2º Deve ser informado à Central de Serviços de TI o encerramento de atividades, contratos ou acordos para que os direitos de acesso às informações e aos recursos de Tecnologia da Informação sejam removidos.

§ 3º Caso o Sistema de Informação possua módulo específico para a manutenção e criação de contas, habilitado para uso do gestor de ativo de informação, a responsabilidade pela criação e manutenção de contas será deste, devendo zelar pela base de usuários de forma que somente pessoas autorizadas tenham acesso ao sistema.

§ 4º O gestor de ativo de informação deve revisar periodicamente os direitos de acesso concedidos, ajustando os perfis de acordo com a necessidade de conhecer do usuário.

Art. 21. O chamado registrado que originou a solicitação de acesso deverá ser respondido, após a conclusão do serviço, com a especificação da liberação do acesso ao ativo da informação, o usuário e a senha de acesso inicial, juntamente com as instruções para a alteração desta após o primeiro acesso.

Art. 22. Os novos sistemas desenvolvidos pela Secretaria de Tecnologia da Informação (STI) devem:

I - possuir log com o registro de acesso dos usuários;

II - ser acessados, preferencialmente, via certificado digital ou integrados ao serviço de autenticação de usuários do TRE-RO;

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

IV - exibir as seguintes informações quando o procedimento de entrada (logon) ocorrer com sucesso:

a) data e hora do último logon com sucesso;

b) detalhes de qualquer tentativa de logon sem sucesso, desde o último procedimento realizado com sucesso.

Art. 23. Todos os acessos à informação devem ser registrados para fins de auditoria em servidor de logs dedicado.

Art. 24. O log de acesso de todos os serviços de TI deve ser armazenado por um período não inferior a 05 (cinco) anos e seus registros devem conter, no mínimo:

I - identificação do usuário;

II - datas e horários de entrada (logon) e saída do sistema (logoff);

III - identificação da estação de trabalho que originou o acesso;

IV - registros das tentativas de acesso (aceitas e rejeitadas) aos sistemas;

V - quando for o caso, as informações acerca dos recursos computacionais, aplicativos, arquivos de dados e utilitários utilizados e que tipos de operações foram efetuadas.

Art. 25. As contas de usuário devem:

I - ser bloqueadas ou desativadas caso não sejam utilizadas por um período maior que 03 (três) meses ou ainda em caso de identificação de comprometimento da segurança da informação;

II - ter uma limitação de 05 (cinco) tentativas de logon sem sucesso, sendo que após a quinta tentativa mal sucedida o sistema deve forçar um tempo de espera antes de permitir novas tentativas.

Art. 26. As estações de trabalho devem ser configuradas para ter:

I - bloqueio automático de tela em casos de períodos de inatividade e, para restaurar a sessão, o usuário deverá ser obrigado a fornecer novamente suas credenciais de acesso;

II - restrição de sessões concorrentes, impedindo que um usuário, sem privilégios, possa acessar a rede a partir de mais de uma estação de forma simultânea.

Art. 27. Não haverá criação de contas genéricas para usuários, excetuando-se os casos de necessidade justificada e acompanhada de parecer do Gestor de Segurança da Informação acerca da possibilidade de aceitação dos riscos associados.

Parágrafo único. Não devem existir contas duplicadas de acesso para os usuários, excetuando-se as contas com privilégio administrativo.

Art. 28. Os direitos de acesso privilegiados, como acesso de administradores dos recursos de TI, devem ser identificados e registrados.

§ 1º O perfil de administrador deve ser concedido à conta específica do usuário e não deverá existir conta genérica compartilhada de administrador.

§ 2º O registro de conta de acesso com perfil de administrador somente deve ser concedido a usuários da STI que necessitem deste perfil no desempenho de suas tarefas na administração dos recursos de TI, excetuando-se os casos de necessidade justificada e acompanhada de parecer do Gestor de Segurança da Informação acerca da possibilidade de aceitação dos riscos associados.

Art. 29. Serão instalados no parque computacional do TRE-RO somente os softwares homologados pela STI.

Art. 30. Apenas servidores da STI, que possuam conta de acesso com perfil de administrador, estão autorizados a realizar instalações de softwares em estações de trabalho do Tribunal.

§ 1º Os usuários que não possuírem o perfil previsto no caput somente poderão realizar instalação de software com autorização expressa da STI, sob pena de responsabilização funcional.

§ 2º O acesso a utilitários de segurança, como editores, compiladores, softwares de manutenção, monitoramento, auditoria e diagnóstico, deve ser restrito a um número mínimo de usuários previamente autorizados.

SEÇÃO II

DA POLÍTICA DE SENHAS

Art. 31. Todos os sistemas ou serviços de informação devem ter seu acesso restrito e controlado através do uso de senhas, token ou mecanismo de autenticação similar.

Art. 32. A senha de acesso do usuário deverá ser secreta, de uso pessoal e intransferível e para que a senha tenha qualidade é necessário atentar para as seguintes recomendações:

I - Não utilizar senhas com menos de 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;

IV - Evitar usar a senha de uso pessoal para senhas de uso profissional.

Art. 33. 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. 34. Sempre que houver indicação de possível comprometimento da senha, deverá ser realizada a sua alteração.

Art. 35. O sistema de gerenciamento de senha 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, conforme definição em norma complementar;

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 - Modificar senhas temporárias no primeiro acesso ao sistema ou serviço de informação.

SEÇÃO III

DOS PROCEDIMENTOS SEGUROS DE ENTRADA NO SISTEMA

Art. 36. O procedimento adequado de entrada no sistema (login) deve atender às seguintes recomendações:

I - Encerrar sessões inativas após um período definido de inatividade;

II - Restringir os tempos de conexão nos sistemas para sessões ativas em períodos prolongados, fornecendo segurança adicional e reduzindo a janela de oportunidade para acesso não autorizado.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 37. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação e Comunicação deste Tribunal.

Art. 38. A revisão desta Política de Controle de Acesso Físico e Lógico relativos à Segurança das Informações e Comunicações ocorrerá sempre que se fizer necessária ou conveniente para este Tribunal, não excedendo o período máximo de 2 (dois) anos.

Art. 39. Esta Política deverá ser publicada no portal de intranet do Tribunal pela respectiva Comissão de Segurança da Informação e Comunicação.

Art. 40. O descumprimento desta Política será objeto de apuração pela unidade competente do Tribunal e sujeito à aplicação das penalidades cabíveis a cada caso.

Art. 41. Esta resolução entrará em vigor na data de sua publicação.

Tribunal Regional Eleitoral - RO -

Porto Velho – RO, 14 de dezembro de 2017.

Desembargador ROWILSON TEIXEIRA – Presidente e Relator

Desembargador WALTER WALTENBERG SILVA JUNIOR – Vice-Presidente e Corregedor Regional Eleitoral

Juiz GLODNER LUIZ PAULETTO

Juíza ROSEMEIRE CONCEIÇÃO DOS SANTOS PEREIRA DE SOUZA

Juiz FLÁVIO FRAGA E SILVA

Juíza ANDRÉA CRISTINA NOGUEIRA

Juiz PAULO ROGÉRIO JOSÉ