TRIBUNAL REGIONAL ELEITORAL DO ACRE

INSTRUÇÃO NORMATIVA Nº 38, DE 17 DEZEMBRO DE 2018

Dispõe sobre a instituição da Política de Controle de Acesso Físico e Lógico relativos à Segurança da Informação do Tribunal Regional Eleitoral do Acre.

A DESEMBARGADORA REGINA CÉLIA FERRARI LONGUINI, PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO ACRE, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de assegurar a integridade e a disponibilidade das informações, como preconizado pela Resolução TRE-AC nº 1.716/2017, que estabelece a Política de Segurança da Informação da Justiça Eleitoral do Acre;

CONSIDERANDO as orientações de controles de segurança da informação dispostas na norma ISO NBR/IEC 27002:2013, às quais esta Política de Controle de Acesso Físico e Lógico está alinhada;

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,

RESOLVE:

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

CAPÍTULO I
DOS CONCEITOS E DEFINIÇÕES

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

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

2. **Acesso lógico**: é o acesso aos sistemas e ativos de informação.

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

4. **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 eles têm acesso.

5. **Autenticação de multifatores**: utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema.

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

7. **Bloqueio de acesso**: processo que tem por finalidade suspender o acesso.

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

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

10. **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.

11. **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.

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

13. **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.

14. **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.

15. **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 de processamento.

Art. 4º O acesso deverá ser concedido aos usuários deste Tribunal atendendo aos princípios 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 da Informação é:

1. Estabelecer diretrizes para implementação de controles de acesso físico e lógico;

2. Preservar os ativos de informação; e,

3. 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 Eleitoral, 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.

Parágrafo único. Todos 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 deverá definir o perímetro de segurança física para proteção tanto das instalações de processamento da informação (*Datacenter*) , bem como as demais áreas que contenham informações críticas ou sensíveis.

Art. 8º As instalações do *Datacenter* deverão atender às seguintes diretrizes:

1. 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;

2. 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;

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

4. Portas corta-fogo com sistema de alarme que sejam monitoradas e funcionem de acordo com os códigos locais de prevenção de incêndios e de falhas;

5. 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;

6. 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;

7. Possua múltiplas alimentações de energia elétrica e telecomunicações, com rotas físicas diferentes;

8. Instalação de iluminação e comunicação de emergência;

9. 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* deverão ser estabelecidas pela Comissão de Segurança da Informação, observadas as legislações vigentes.

SEÇÃO II

DOS EQUIPAMENTOS DE PROCESSAMENTO E ARMAZENAMENTO

Art. 10. Para evitar perdas, danos, furtos, ou comprometimento de ativos e interrupção das operações da organização, o Tribunal deverá seguir as seguintes diretrizes:

1. 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;

2. 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;

3. Adotar controles para evitar a retirada de equipamentos deste Tribunal sem prévia autorização.

SEÇÃO III

DA SEGURANÇA DO CABEAMENTO

Art. 11. 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:

1. 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;

2. Os cabos de energia elétrica devem ser segregados dos cabos de comunicação, para evitar interferências;

SEÇÃO IV

DA MANUTENÇÃO EXTERNA DOS EQUIPAMENTOS

Art. 12. A manutenção dos equipamentos de processamento de informações deverá seguir as seguintes diretrizes:

1. A manutenção e os consertos dos equipamentos sejam realizados somente por pessoal de manutenção autorizado;

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

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

4. 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. 13. Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados, pela área técnica da STI, antes da reutilização ou descarte, para assegurar que todos os dados sensíveis e *softwares* licenciados tenham sido removidos ou sobre gravados com segurança.

§1º Os equipamentos deverão ser inspecionados, pela área técnica da STI, 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 sobre gravadas por meio de técnicas que tornem as

informações originais irrecuperáveis.

SEÇÃO VI
DA POLÍTICA DE MESA LIMPA E TELA LIMPA

Art. 14. 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. 15. As operações de criação e exclusão/inativação de usuários da rede local (autenticação e/ou correio eletrônico) devem ser solicitadas, por meio do sistema de *service desk*:

§ 1º. Pela Coordenadoria de Gestão de Pessoas para os magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo e estagiários.

§ 2º. Pela fiscalização administrativa dos contratos para os colaboradores e prestadores de serviços.

§ 3º. Pela Diretoria-Geral para os demais casos.

Art. 16. Cabe ao chefe imediato solicitar, por meio do sistema de *service desk*, a criação de usuário de sistema para os servidores lotados em sua unidade, informando quais os sistemas/serviços e quais os perfis de acesso que os mesmos deverão possuir.

§ 1º. O perfil de acesso do usuário aos sistemas ou serviços de informação deverá ser mantido restrito ao desempenho de suas atividades.

§ 2º. O gestor do ativo de informação será responsável pela autorização do direito de acesso.

Art. 17. Os usuários deverão possuir identificação única e exclusiva para permitir relacioná-la às suas ações e responsabilidades.

Art. 18. Compete à chefia imediata informar, antecipadamente, aos responsáveis estabelecidos no artigo 15 deste normativo a movimentação ou o desligamento de qualquer usuário alocado em sua unidade, dadas as implicações na manutenção de direitos de acesso aos ativos de informação.

Art. 19. Os direitos de acesso dos usuários deverão ser revistos, pelo gestor do ativo de informação, em intervalos regulares e depois de qualquer mudança de função, alteração de lotação ou desligamento.

§ 1º. Compete ao gestor do ativo de informação realizar a revisão de direitos de acesso ao ativo sob sua responsabilidade.

§ 2º. Compete ao chefe imediato realizar a revisão de direitos de acesso dos usuários sob sua chefia.

SEÇÃO II
DA POLÍTICA DE SENHAS

Art. 20. Os sistemas ou serviços de informação, considerados passíveis de controle de acesso pelo gestor do ativo, devem ter seu acesso restrito e controlado através do uso de senhas, *token* ou mecanismo de autenticação similar.

Art. 21. A senha de acesso do usuário deverá ser secreta, de uso pessoal e intransferível. Para definição da senha de acesso, o usuário deverá considerar as seguintes recomendações:

1. Usar números, letras, alternando-as entre maiúsculas e minúsculas, e caracteres especiais, como $@#&%;

2. 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;

3. 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;

4. Não usar a senha de uso pessoal para senhas de uso profissional.

Art. 22. 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. 23. Sempre que houver indicação de possível comprometimento da senha, deverá ser realizada a sua alteração.

Art. 24. O sistema de gerenciamento de senha deverá:

1. Permitir que os usuários selecionem e modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros;

2. Forçar as mudanças de senha a intervalos regulares, conforme necessidade;

3. Manter um registro das senhas anteriores utilizadas e bloquear a reutilização;

4. Armazenar e transmitir as senhas de forma protegida;

5. Não mostrar as senhas na tela quando forem digitadas;

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

SEÇÃO III

DOS PROCEDIMENTOS SEGUROS DE ENTRADA NO SISTEMA

Art. 25. O procedimento adequado de entrada no sistema (*login)* deve atender às seguintes recomendações:

1. Não fornecer mensagens de ajuda durante o procedimento de entrada que poderiam auxiliar um usuário não autorizado;

2. Validar informações de entrada no sistema somente após todos os dados estarem completamente preenchidos;

3. No caso de erro, não indicar qual parte do dado de entrada está correta ou incorreta;

4. Bloquear o sistema após, no máximo, cinco tentativas de entrada no sistema;Registrar tentativas de acesso ao sistema, sem sucesso e bem sucedidas;

5. Quando da entrada no sistema, mostrar as seguintes informações:

6. data e hora da última entrada no sistema com sucesso;

7. detalhes de qualquer tentativa sem sucesso de entrada no sistema desde o último acesso com sucesso;

8. Não mostrar a senha que está sendo informada;

9. Não transmitir senhas em texto claro pela rede;

10. Encerrar sessões inativas após um período definido de inatividade.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 26. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação deste Tribunal.

Art. 27. A revisão desta Política de Controle de Acesso Físico e Lógico relativos à segurança da informação ocorrerá sempre que se fizer necessário ou conveniente para este Tribunal, não excedendo o período máximo de 3 (três) anos.

Art. 28. Esta política deverá ser publicada no portal de intranet do Tribunal pela Comissão de Segurança da Informação.

Art. 29. O descumprimento desta política será objeto de apuração pela unidade competente do Tribunal e consequente aplicação das penalidades cabíveis a cada caso.

Art. 30. Esta instrução normativa entrará em vigor na data de sua publicação e deverá ser implantada, gradativamente.

Rio Branco, 17 de dezembro de 2018.

Documento assinado eletronicamente por **Regina Célia Ferrari Longuini**, **Presidente**, em 19/12/2018, às 14:56, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-ac.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0252231** e o código CRC **B171F561**.