Tribunal Regional Eleitoral
do Espírito Santo

Sede: Vitória/ES
Av. João Batista Parra, 575
Praia do Suá - Vitória - ES
CEP 72620-000
Tel.: (27) 2121.8595
Endereço eletrônico:
www.tre-es.jus.br

Comissão de Segurança da Informação

NSI-006	V1.0 - FEV 2022	SEGURANÇA DA INFORMAÇÃO

Acesso Remoto

Referência(s):

Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)

Resolução CNJ 396/2021 – ENSEC-PJ

Resolução TSE 23.644/2021 – PSI/JE

Resolução TSE 23.650/2021 – Política Geral de Privacidade e Proteção de Dados Pessoais

Palavras Chave: segurança, norma, acesso, remoto. | 05 páginas

1. Prefácio

A presente norma está alinhada às diretrizes de Segurança da Informação e dos Dados Pessoais estabelecidas na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) e na Política de Segurança da Informação da Justiça Eleitoral (PSI-JE).

2. Objetivo

Estabelecer as diretrizes de segurança para o acesso remoto aos recursos tecnológicos do Tribunal Regional Eleitoral do Espírito Santo.

3. Abrangência

Esta norma se aplica a todos os usuários que fazem uso dos recursos tecnológicos do Tribunal Regional do TRE/ES através de computadores corporativos que não estão fisicamente conectados à rede local.

4. Disposições Gerais

4.1. O acesso remoto à rede local dar-se-á única e exclusivamente por portal seguro, com registro de acesso.

4.2. O acesso remoto será permitido a magistrados, servidores, estagiários e colaboradores previamente cadastrados.

4.3. Cabe à Comissão de Segurança da Informação deliberar sobre os dias e horários em que o acesso remoto estará disponível, considerando as necessidades de trabalho do Tribunal.

5. Dos requisitos de segurança para o acesso remoto

5.1. O acesso remoto será permitido apenas através de equipamentos corporativos previamente configurados e cadastrados. É vedado o uso de equipamentos pessoais.

5.1.1. São requisitos de segurança dos equipamentos corporativos utilizados para trabalho remoto:

5.1.1.1. Bloqueio de instalação de aplicativos;

5.1.1.2. Antivírus corporativo instalado, que permita atualizações automáticas;

5.1.1.3. Certificado digital instalado para cada usuário apto a utilizar o equipamento para acesso remoto; e

5.1.1.4. Software de suporte remoto corporativo habilitado.

5.2. O acesso remoto aos recursos computacionais é permitido somente em território nacional.

5.2.1. Excepcionalmente, o servidor poderá requerer à Administração, com antecedência mínima de 30 (trinta) dias, o uso no exterior, indicando a justificativa, o país e o período. Adicionalmente, outras informações podem ser exigidas pela área técnica e devem ser fornecidas, sob pena de o acesso não ser liberado.

5.2.2. Identificada alguma ameaça iminente, outras restrições regionais podem ser adotadas pela área técnica, com imediata comunicação aos usuários.

5.3. O acesso remoto ao portal seguro será permitido somente mediante o uso de múltiplo fator de autenticação, conforme regras estabelecidas pela área técnica.

6. Do uso remoto dos equipamentos corporativos

6.1. Os equipamentos corporativos são de uso exclusivo dos magistrados, servidores, estagiários e colaboradores previamente cadastrados na rede corporativa do Tribunal, estritamente para exercício de suas atribuições funcionais.

6.1.1. Os equipamentos corporativos destinados ao uso em trabalho remoto não podem ser cedidos ou emprestados a terceiros, incluindo familiares e amigos, mesmo que para pequenas tarefas.

6.2. É vedada a instalação ou a tentativa de instalação de qualquer programa, aplicativo ou serviço pelo usuário do equipamento.

6.2.1. Havendo necessidade de uso de algum programa específico, a área técnica deve ser consultada e, se for o caso, providenciar o suporte para a instalação.

6.3. Todas as atividades relativas à segurança do equipamento corporativo são passíveis de registro, incluindo, dentre outras:

a) Instalação ou tentativa de instalação de programas e/ou serviços;
b) Sítios de internet visitados;
c) Termos consultados em site de pesquisa;
d) Tentativa de alteração de configuração;

e) Uso de dispositivos externos;
f) Tentativa de uso de credenciais administrativas;
g) Tentativa de eliminação de registros de segurança;

6.4. É vedado o uso do equipamento corporativo destinado ao trabalho remoto para tentar comprometer a segurança da rede de dados do Tribunal.

6.5. Em caso de perda ou roubo do equipamento corporativo, a área técnica do Tribunal deve ser imediatamente informada para que efetue o bloqueio do acesso remoto através daquele equipamento.

7. Da Gestão de Segurança do serviço de acesso remoto

7.1. A área técnica responsável pela gestão do serviço de acesso remoto deve efetuar atualizações periódicas de segurança nos equipamentos e softwares que sustentam o serviço de acesso remoto.

7.2. A área técnica de microinformática e gestão de serviços deve propor e aplicar soluções visando aprimorar a segurança dos equipamentos usados para o acesso remoto dos magistrados, servidores e colaboradores.

7.3. Com o intuito de promover a segurança da rede, identificada alguma infração a esta norma ou qualquer situação de risco iminente para a infraestrutura tecnológica, a área técnica responsável pela gestão do serviço de acesso remoto poderá bloquear e/ou limitar o acesso remoto de um usuário ou grupo de usuários à rede de comunicação de dados.

7.3.1. A área técnica deverá produzir relatório com a motivação do bloqueio e submeter à Comissão de Segurança da Informação para providências cabíveis.

7.4. Com o intuito de promover a segurança da rede, em situações iminentes de ataques ou identificação de vulnerabilidades críticas de alto impacto, a área técnica responsável pela gestão do serviço de acesso remoto poderá bloquear e/ou limitar o serviço de acesso remoto, comunicando imediatamente à Comissão de Segurança da Informação e à Administração do Tribunal.

7.5. O acesso remoto poderá ser totalmente vedado nos dias que antecedem as eleições oficiais até que a totalização e a divulgação dos resultados tenham sido concluídas.

8. Das responsabilidades

8.1. Da Comissão de Segurança da Informação:

8.1.1. Deliberar sobre dias e horários em que o acesso remoto será permitido.

8.1.2. Deliberar sobre as ações a serem adotadas em caso de desrespeito aos termos desta norma.

8.1.3. Manter atualizados os dispositivos desta norma.

8.2. Da área técnica responsável pela gestão do acesso remoto:

8.2.1. Definir e dar ciência aos usuários quanto à forma de autenticação de múltiplo fator utilizada para acesso remoto.

8.2.2. Bloquear e/ou limitar o acesso remoto de um usuário ou grupo de usuários em caso de identificação de violação desta norma.

8.2.3. Bloquear e/ou limitar o serviço de acesso remoto em caso de risco iminente de ataque.

8.2.4. Apoiar tecnicamente a Comissão de Segurança da Informação nas deliberações sobre regras para o acesso remoto.

8.2.5. Efetuar a gestão de segurança do acesso remoto.

8.2.6. Informar à Comissão de Segurança da Informação violações à norma identificadas, produzindo relatório técnico sobre a infração.

8.2.7. Comunicar aos usuários quanto à realização de manutenções programadas que inviabilizem o acesso remoto.

8.2.8. Adotar providências para prover e manter atualizados as ferramentas e os procedimentos de acesso remoto, a fim de aumentar a segurança da rede.

8.3. Da área técnica responsável pela microinformática e gestão de serviços de TIC:

8.3.1. Propor e aplicar soluções visando aprimorar a segurança dos equipamentos usados para o acesso remoto dos servidores e magistrados.

8.3.2. Prestar o suporte remoto aos equipamentos corporativos usados em trabalho remoto, exclusivamente por meio de ferramenta de suporte corporativa adotada pelo Tribunal.

8.4. Dos usuários do serviço de acesso remoto:

8.4.1. Comunicar imediatamente a área técnica a respeito de qualquer tipo de ocorrência – perda, roubo, dano, invasão, etc – com o equipamento corporativo usado para trabalho remoto.

8.4.2. Respeitar integralmente os dispositivos desta norma no manuseio do equipamento corporativo e no uso do serviço de acesso remoto.

9. Das disposições finais

9.1. A liberação do acesso remoto e o empréstimo de equipamentos para estagiários ficam sujeitos à autorização e regramento próprios, estabelecidos pela Administração.

9.2. Os casos omissos nesta norma deverão ser resolvidos pela Comissão de Segurança da Informação.

10. Da vigência e atualização

10.1. Esta norma operacional entra em vigor a partir da data de sua publicação e sua atualização ocorrerá sempre que se fizer necessária.