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

Comitê Gestor de
Segurança da Informação

NSI-001	V3.0 - FEV 2022	SEGURANÇA DA INFORMAÇÃO

Acesso à Internet

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, diretrizes internet, rede. | 08 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. Definições

- **Ferramenta sistêmica de segurança de rede:** solução integrada de *hardware* e *software* instalada e configurada para monitorar o acesso à Internet e aplicar políticas de controle visando a segurança e a disponibilidade dos ativos de TIC da Justiça Eleitoral.
- **Cache de navegador web:** conjunto de itens vistos ou descarregados enquanto se navega na Internet, armazenados localmente do computador, com objetivo de acelerar o tempo de exibição das páginas web em caso de uma segunda visita.
- **Conteúdo inapropriado ou ilegal:** Todo e qualquer conteúdo que represente infração à esta norma ou infrinja as leis vigentes.
- **Ativos de TIC:** conjunto de equipamentos, softwares e bases de dados que integram a infraestrutura tecnológica do Tribunal.

3. Objetivo

Estabelecer as diretrizes de proteção e responsabilidades relativas ao uso da Internet provida pelo Tribunal Regional Eleitoral do Espírito Santo.

4. Abrangência

Esta norma se aplica a todos os usuários que fazem uso da Internet, permanente ou temporariamente, através da infraestrutura tecnológica disponibilizada pelo TRE/ES.

5. Disposições gerais

5.1. O acesso à Internet é permitido apenas para navegação em sítios cujo conteúdo esteja adequado aos termos desta norma.

5.2. A possibilidade de acesso a qualquer serviço da Internet não significa a existência de autorização para acessá-lo.

6. Das permissões e formas de acesso

6.1. O acesso à Internet dar-se-á através de uma conta de usuário que possibilite identificar, individualmente, seu proprietário.

6.1.1. A conta é de uso pessoal e intransferível, sendo o usuário responsável por todas as atividades realizadas através de sua chave de acesso.

6.2. Os usuários internos, ao serem cadastrados e habilitados na rede local do TRE/ES, terão acesso à Internet liberado.

6.2.1. Quando o uso da Internet não for necessário ao desenvolvimento das atividades, os gestores poderão solicitar, por meio da CESTIC, o bloqueio de acesso de usuários sob sua supervisão. Da mesma forma, poderão solicitar o bloqueio de sítios e aplicações web não relacionados às atividades desenvolvidas.

6.3. Havendo infraestrutura tecnológica disponível, usuários externos, identificados e cadastrados na recepção da sede do Tribunal, terão acesso à Internet com uso de seus dispositivos pessoais.

7. Do monitoramento e auditoria

7.1. Os acessos à Internet através da rede interna do Tribunal devem ser monitorados e registrados individualmente, de modo a detectar violações a esta norma, respeitando-se as limitações quanto ao sigilo de informações classificadas ou protegidas por lei.

7.1.1. O registro deverá conter, no mínimo: identificação precisa do usuário de rede; data/hora de início das conexões e dos sítios acessados. Adicionalmente, poderão

ser registrados o tipo, a quantidade de tráfego gerado e outras informações necessárias para a realização de auditoria.

7.2. O prazo mínimo para retenção dos *logs* de acesso será de 06 (seis) meses.

7.3. O Presidente e o Corregedor poderão solicitar ao setor técnico o exame, sem aviso prévio ao usuário, do conteúdo de *cache* de navegadores *web*, favoritos, histórico de sites visitados, configurações dos *softwares* e outras informações armazenadas ou transmitidas pelos computadores do TRE/ES.

7.4. Os gestores poderão solicitar formalmente à Comissão de Segurança de Informação relatório relativo a seus subordinados, com os registros de acesso à Internet previstos no subitem 7.1.

8. Uso aceitável da Internet

8.1. O acesso à Internet é permitido em sítios que sejam fontes de informação necessária à execução das atividades do TRE/ES.

8.2. É permitido o uso de serviços pessoais prestados através da Internet, tais como banco on-line, reservas de passagens, serviços de órgãos públicos, entre outros, limitados ao estritamente necessário;

8.3. É permitido o uso de serviços privados de correio eletrônico, vedado o compartilhamento de informações corporativas, dados pessoais tratados pelo Tribunale o redirecionamento automático de mensagens institucionais para contas pessoais.

8.4. É permitido o uso de serviços homologados de armazenamento de arquivos em nuvem, ressalvada a manutenção de uma cópia dos arquivos importantes na rede local.

8.4.1. A divulgação dos serviços homologados será feita através da página da Comissão de Segurança de Informação na Intranet.

8.5. Não cabe ao setor técnico do Tribunal prestar suporte ao uso dos serviços previstos nos itens 8.2 e 8.3.

8.6. Durante a navegação, ao verificar que o sítio acessado contém conteúdo inapropriado ou ilegal, o usuário deverá abandonar o sítio, devendo informar o setor técnico acerca da impropriedade ou ilegalidade do conteúdo, por meio de abertura de chamado técnico na CESTIC, para fins de bloqueio do referido endereço eletrônico.

9. Das vedações em função da segurança dos ativos de TIC

9.1. É permanentemente vedada a utilização da Internet para acessar:

9.1.1. Sítios e aplicações classificados com grau de risco crítico pela ferramenta sistêmica do TRE/ES;

9.1.2. Sítios e ferramentas que permitem burlar regras de bloqueio e navegar anonimamente na Internet;

9.1.3. Sítios com informações voltadas a atividades computacionais maliciosas, que contenham conteúdo criminoso ou ilegal, ou que façam sua apologia, incluindo os de pirataria ou que divulguem número de série para registro de *softwares;*

9.1.4. Serviços de armazenamento de arquivos em nuvem não homologados.

9.2. Em hipótese alguma proceder-se-á à liberação de sítios bloqueados em função de segurança.

10. Das vedações em função de inadequação de conteúdo e tráfego elevado

10.1. É vedada a utilização da Internet para acessar:

10.1.1. Sítios com materiais relativos a sexo, pornografia, nudez, racismo, violência, incitação ao ódio e invasão de computadores;

10.1.2. Sítios e aplicações de jogos e simulações de mundos virtuais;

10.1.3. Redes sociais;

10.1.4. Sítios e aplicações de apostas;

10.1.5. Sítios e aplicações de troca de mensagens, envio de SMS, comunicação de voz sob IP e conferência *web*;

10.1.6. Sítios e aplicações de compartilhamento de arquivos ponto a ponto, vídeos e músicas;

10.1.7. Sítios e aplicações de áudio, vídeo e TV em tempo real;

10.1.8. Aplicações de gerenciamento de *download* e *plugin* de navegadores;

10.1.9. Ferramentas de administração remota de computadores.

10.2. Sítios da Administração Pública devem permanecer com acesso liberado, ainda que possuam aplicações que se enquadrem em alguma das hipóteses acima.

11. Das regras e do bloqueio através de ferramenta sistêmica

11.1. Todos os acessos à Internet através da rede interna do Tribunal serão monitorados pela ferramenta sistêmica de segurança de rede do TRE/ES.

11.2. A ferramenta sistêmica de segurança de rede deverá ser configurada com regras restritivas que reflitam os termos estabelecidos nesta norma.

11.3. A ferramenta sistêmica de segurança de rede aplicará automaticamente regras restritivas a partir de suas listas internas de sítios e aplicações reconhecidamente danosos.

12. Da liberação de sítios e aplicações web

12.1. As demandas de liberação de acesso devem ser apresentadas inicialmente por meio de chamado técnico aberto na Central de Serviços de TIC, com indicação do endereço eletrônico e da justificativa da necessidade.

12.2. O setor técnico responsável pela segurança dos ativos de TIC avaliará o sítio e:

12.2.1. Efetuará a liberação caso verifique que se trata de um sítio que foi classificado de forma equivocada (falso positivo) pela ferramenta sistêmica de segurança de rede;

12.2.2. Efetuará a liberação caso a demanda não traga risco, não comprometa a performance da rede e o conteúdo esteja claramente ajustado à necessidade de trabalho apresentada;

12.2.2.1. Em se tratando de sítio cuja liberação integral comprometa a performance da rede, o setor técnico poderá proceder à liberação parcial, caso seja viável tecnicamente.

12.2.3. Informará o usuário sobre a vedação expressa determinada nesta norma, nos casos de sítios que tenham sido bloqueados em função da segurança dos ativos de TIC;

12.2.4. Procederá ao fechamento do chamado, informando que o pedido deve ser encaminhado ao presidente da Comissão de Segurança da Informação, para ser submetido à apreciação dos integrantes da Comissão, nos demais casos.

12.3. As demandas de liberação de acesso não aprovadas pelo setor técnico devem ser assinadas pelos gestores das unidades e encaminhadas ao presidente da Comissão de Segurança da Informação, para serem submetidas à apreciação em um prazo de até 30 dias.

12.3.1. O presidente da Comissão de Segurança da Informação poderá autorizar a liberação temporária do sítio até que a Comissão aprecie definitivamente a demanda.

12.4. A Comissão de Segurança da Informação poderá determinar justificadamente a liberação, completamente ou em parte, permanentemente ou por período determinado, de qualquer um dos conteúdos dispostos no item 10, bastando formalizar o pedido junto ao setor responsável pela segurança dos ativos de TIC.

12.4.1. As liberações de conteúdo, a justificativa e o período de vigência devem ser publicadas na página da comissão na Intranet.

12.5. Os conteúdos dispostos no item 10 podem ainda ser liberados mediante publicação de normas específicas propostas pela área técnica e aprovadas pela Comissão de Segurança da Informação.

13. Das responsabilidades

13.1. Cabe à Comissão de Segurança da Informação:

13.1.1. Apreciar, no prazo estabelecido, as solicitações de liberação de sítios;

13.1.2. Informar ao setor técnico as decisões referentes à liberação dos sítios;

13.1.3. Manter atualizados os dispositivos desta norma;

13.1.4. Propor apuração de eventual desobediência aos dispositivos desta norma.

13.2. Cabe aos gestores:

13.2.1. Orientar seus subordinados quanto ao uso racional e consciente da Internet e comunicar situações que possam configurar violação a esta norma;

13.2.2. Avaliar e encaminhar à Comissão de Segurança da Informação os pedidos de liberação de sítios necessários às atividades de seus subordinados.

13.3. Cabe ao setor técnico responsável pela segurança dos ativos de TIC:

13.3.1. Definir, implantar e gerenciar a ferramenta sistêmica de segurança de rede;

13.3.2. Monitorar e registrar em *log* o acesso à Internet, de modo a detectar violações a esta norma, respeitando-se as limitações quanto ao sigilo de informações protegidas por lei;

13.3.3. Informar à Comissão de Segurança de Informação violações à norma identificadas;

13.3.4. Apoiar tecnicamente a Comissão de Segurança de Informação nas decisões sobre liberação de acesso a sítios;

13.3.5. Comunicar os usuários quanto à realização de manutenções programadas no serviço que venham a causar indisponibilidade;

13.3.6. Decidir, emergencialmente, sobre a suspensão temporária de usuários que infrinjam qualquer dispositivo desta norma e, se necessário, submeter o caso à Comissão de Segurança da Informação.

13.4. Cabe aos usuários:

13.4.1. Abster-se de utilizar do acesso à Internet para tentar comprometer a segurança (integridade, confidencialidade ou disponibilidade) de computadores, sistemas ou serviços do TRE-ES;

13.4.2. Manter o sigilo de suas credenciais de acesso, a fim de evitar que outros usuários façam uso da Internet com suas credenciais;

13.4.3. Reportar ao setor técnico responsável, por meio da CESTIC, eventuais incidentes que possam afetar a segurança dos ativos de TIC, inclusive dos dados pessoais tratados pelo Tribunal;

13.4.4. Desconectar-se com segurança de sistemas web, utilizando links específicos para este fim, como “Sair”, “Logoff” ou “Desconectar”.

14. Das disposições finais

14.1. Consideram-se gestores, para os fins deste regulamento, o Presidente, o Corregedor, o Diretor-Geral, os Secretários, o Coordenador da Unidade de Auditoria Interna, nos Cartórios Eleitorais, os Juízes Eleitorais.

14.2. Com o intuito de promover a eficiência e o uso racional dos recursos de comunicação de dados, o setor técnico responsável pela segurança dos ativos de TIC poderá bloquear e/ou limitar o acesso a sítios de Internet, priorizando o uso institucional.

14.3. O suporte técnico ao funcionamento e uso do serviço estará disponível regulamente durante o horário de funcionamento da Secretaria do Tribunal.

14.3.1. Excepcionalmente, havendo necessidade, os gestores poderão solicitar autorização da Administração para que o setor técnico preste suporte em outros períodos.

14.4. Os incidentes, indícios de quebra de segurança e denúncias de descumprimento da Política de Segurança da Informação da Justiça Eleitoral, da Política Geral de Privacidade e Proteção de Dados Pessoais e suas normas devem ser encaminhados através da CESTIC.

14.5. No estrito cumprimento de suas funções institucionais e/ou para fins de auditoria autorizada pela Administração, a área técnica poderá ter acesso aos conteúdos vedados, interna ou remotamente, a partir de dispositivos do TRE/ES ou pessoais, sendo obrigatória a identificação individualizada do acesso.

14.6. Ao descumprir qualquer disposição desta norma, o usuário estará sujeito às sanções administrativas, civis e penais aplicáveis ao caso.

14.7. Esta norma entra em vigor na data de sua publicação.