Tribunal Regional Eleitoral
do Espírito Santo

Sede: Vitória/ES
Av. João Baptista Parra, 575
Praia do Suá - Vitória - ES
CEP 29052-123
Tel.: (27) 2121.8595
Endereço eletrônico:
www.tre-es.jus.br

Comissão de Segurança da Informação

NSI-009	V3.0 - FEV-2025	SEGURANÇA DA INFORMAÇÃO

Norma de uso aceitável dos recursos de Tecnologia da Informação

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

Portaria DG/TSE 444/2021, instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral

Portaria nº 456/2021 do TSE, que dispõe sobre o uso aceitável de ativos de TI.

ABNT ISO/IEC 27001 e ABNT NBR ISO/IEC 27002

§ 6º do artigo 37 da Constituição Federal que dispõe sobre a responsabilidade civil objetiva atribuída aos entes estatais

Palavras-Chave: segurança, norma, recursos	13 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. Dos conceitos e definições

- **acesso remoto:** toda conexão estabelecida com a rede do TSE ou Tribunais Eleitorais originada de um ponto externo, fora das dependências do Tribunal ou de suas unidades administrativas;
- **antimalware:** programas informáticos desenvolvidos para prevenir, detectar e eliminar malware de computador;
- **antispam:** serviço de detecção e análise que tem como objetivo bloquear o recebimento de spam;

- **ativos de informação e comunicação:** meios de armazenamento, transmissão e processamento, assim como sistemas de informação, instalações e pessoas que a elas têm acesso;

- **autenticidade:** garantia de veracidade da fonte de informações, por meio da qual é possível confirmar a identidade das pessoas ou entidades que prestam a informação;

- **backup:** cópia de segurança de dados;

- **código malicioso (malware):** termo comumente utilizado para, genericamente, se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel, cujos tipos específicos são vírus, worm, bot, spyware, backdoor, cavalo de troia e rootkit;

- **confidencialidade:** garantia de que a informação esteja acessível somente a pessoas autorizadas;

- **credenciais de acesso:** permissões concedidas por autoridade competente, que habilitam determinada pessoa, sistema ou organização ao acesso à informação ou recurso. A credencial pode ser física ou lógica para identificação de usuários;

- **dados pessoais:** informações que permitem identificar um indivíduo, direta ou indiretamente, inclusive sobre crianças e adolescentes e informações pessoais sensíveis, na forma estabelecida na LGPD;

- **disponibilidade:** garantia de que a informação esteja disponível a todas as pessoas autorizadas a utilizá-la;

- **estação de trabalho:** conjunto de hardware e software fornecido ao usuário para que possa executar suas atribuições;

- **geolocalização:** recurso tecnológico que permite localizar qualquer objeto ou pessoa, por meio da sua posição geográfica, detectada automaticamente por um sistema de coordenadas;

- **integridade:** garantia de que a informação seja mantida íntegra, sem modificações indevidas, acidentais ou propositais;

- **IPTV:** método de transmissão de sinais televisivos através de redes IP;
- **phishing:** técnica de fraude utilizada por criminosos para roubar senhas de banco e outras informações pessoais, usando-as posteriormente de maneira fraudulenta;
- **princípio do menor privilégio:** premissa de fornecer permissões e direitos mínimos necessários e suficientes para um usuário realizar suas atividades, por tempo limitado;
- **recursos de tecnologia da informação e comunicação:** computadores, tablets, smartphones, intranet, e-mail institucional, serviço de mensageria institucional, sistemas de informação e quaisquer outros ativos de tecnologia do TRE-ES;
- **Rede Corporativa de Comunicação de Dados da Justiça Eleitoral (RCJE):** conjunto formado pelos segmentos da Rede Nacional, da Rede Regional do Tribunal Superior Eleitoral, dos Tribunais Regionais Eleitorais, dos Cartórios Eleitorais e de suas Redes Locais;
- **rede de computadores:** também conhecida por rede corporativa. Conjunto de computadores, funcionalidades e outros dispositivos, de propriedade do Tribunal que, ligados em uma rede de comunicação de dados, possibilitam a prestação de serviços de TI;
- **risco:** combinação da probabilidade de ocorrência de um evento e de suas consequências;
- **site (ou sítio):** conjunto de páginas web organizadas e acessíveis a partir de um URL da rede interna (Intranet) ou da Internet;
- **spam:** prática de envio em massa de e-mails não solicitados;
- **usuário colaborador:** prestador de serviço terceirizado, estagiário ou qualquer outro colaborador da Justiça Eleitoral que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo Tribunal;
- **usuário externo:** servidor inativo, pessoa física ou jurídica que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas no âmbito da Justiça Eleitoral e que não se enquadre nas definições de usuário interno e usuário colaborador;

- **usuário interno:** autoridade ou servidor ativo do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo órgão.

3. Objetivo

Estabelecer diretrizes para o uso dos recursos de tecnologia da informação no âmbito do Tribunal Regional Eleitoral do Espírito Santo (TRE-ES).

4. Escopo

4.1. Este normativo 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 comunicação da Justiça Eleitoral.

4.1.1. Os contratos firmados pelo Tribunal onde haja disponibilização de mão de obra alocada devem prever, como condição, que os colaboradores terceirizados conheçam e aceitem os termos desta norma.

4.1.2. Os contratos/convênios para contratação de estagiários devem prever como condição o conhecimento e aceite dos termos desta norma.

5. Dos princípios

Esta norma tem como princípio norteador a garantia da segurança, integridade, confidencialidade, autenticidade e disponibilidade dos ativos de informação e comunicação.

6. Das disposições gerais

6.1. Respeitado o disposto na Lei Federal nº 9.609, de 19 de fevereiro de 1998, que trata da propriedade intelectual de programa de computador, e ressalvadas as exceções previstas em contratos e convênios, são de propriedade do Tribunal os programas desenvolvidos, para os fins institucionais, pelos usuários elencados **no item 4.1**.

6.2. Os recursos de Tecnologia da Informação disponibilizados aos usuários destinam-se exclusivamente à execução de atividades da Justiça Eleitoral ou a ela diretamente correlatas.

6.2.1. A utilização será monitorada, podendo ser objeto de auditoria.

6.3. Os recursos de TI não deverão ser utilizados para acessar, criar, transmitir, distribuir ou armazenar conteúdo que desrespeite as leis e regulamentações, especialmente aquelas referentes aos crimes cibernéticos, contra a pessoa, contra os costumes, contra a ética e a decência.

6.3.1. O uso indevido é passível de sanção disciplinar na forma da lei.

6.4. Compete ao usuário zelar pela integridade e conservação dos ativos de Tecnologia da Informação em seu poder, responsabilizando-se por eventuais danos causados aos ativos.

7. Das restrições de acesso aos recursos de tecnologia da informação

7.1. O acesso aos recursos de tecnologia da informação e comunicação pode ser limitado, a fim de garantir a segurança cibernética do órgão. Poderão ser restringidos:

7.1.1. os horários de acesso;

7.1.2. a geolocalização; e

7.1.3. os dias específicos (eleição, feriado, fim de semana etc.)

7.2. As restrições deverão ser propostas pela área técnica responsável pela segurança cibernética, aprovadas pela Comissão de Segurança da Informação e submetidas à apreciação da Administração.

7.2.1. Excepcionalmente e justificadamente, a área técnica responsável pela segurança cibernética poderá proceder à restrição de acesso aos recursos. Neste caso, submeterá imediatamente o caso à Comissão de Segurança da Informação, que poderá cancelar a restrição ou ratificá-la, encaminhando-a em seguida para apreciação da Administração.

8. Das estações de trabalho

8.1. Todo servidor da Justiça Eleitoral terá, em seu posto de trabalho, acesso a uma estação de trabalho destinada à execução de atividades da Justiça Eleitoral ou a ela diretamente correlatas.

8.1.1. Aos estagiários e aos terceirizados será disponibilizado, quando possível e pertinente, acesso a uma estação de trabalho.

8.2. As estações de trabalho devem possuir configurações de hardware e software padronizadas com, no mínimo, os seguintes requisitos de segurança:

8.2.1. Sistema operacional com suporte ativo para recebimento automático de atualizações de segurança.

8.2.2. Softwares instalados configurados para receber atualização de forma automática, sempre que tecnicamente viável.

8.2.3. Software antimalware instalado, ativado, permanentemente atualizado e configurado para realizar verificação automática das mídias removíveis.

8.2.4. Reprodução automática de mídias removíveis desativada.

8.2.5. Instalação de softwares permitida somente para administradores.

8.2.6. Bloqueio automático de tela por inatividade, com restauração da sessão somente por meio do uso de credencial de acesso válida.

8.2.7. Apenas softwares de navegação web e provedores de e-mail suportados podem ser instalados, e devem ser atualizados para a versão mais recente disponível.

8.3. As estações de trabalho receberão somente softwares:

8.3.1. Livres, homologados pela área técnica, que possuam atualizações disponibilizadas periodicamente, com intervalos não superiores a 4 meses;

8.3.2. Corporativos, adquiridos pelo Tribunal, com licença de uso válida, com atualizações e suporte ativo do fornecedor.

8.4. A fim de preservar a segurança e a integridade da rede de comunicação de dados, a área técnica poderá desabilitar dispositivos de hardware e software nativos das estações de trabalho.

8.5. São deveres do usuário relativos às estações de trabalho:

8.5.1. Bloquear o equipamento sempre que se ausentar do seu posto de trabalho;

8.5.2. Informar ao setor técnico quando identificar qualquer violação da integridade física do equipamento;

8.5.3. Solicitar a desinstalação de softwares ou serviços que não forem mais úteis ao desempenho das atividades institucionais.

8.6. É vedado ao usuário em relação às estações de trabalho:

8.6.1. Compartilhar pastas na rede local;

8.6.2. Abrir fisicamente o equipamento para qualquer fim;

8.6.3. Permitir o uso do equipamento por pessoas estranhas aos quadros da Justiça Eleitoral;

8.6.4. Alterar qualquer configuração de hardware ou software;

8.6.5. Instalar ou desinstalar, por conta própria, quaisquer tipos de software nas estações de trabalho.

8.7. Caso seja necessário um novo serviço ou software não disponível na estação de trabalho, o gestor da área de negócio deverá solicitá-lo à área técnica por meio do canal de comunicação regularmente estabelecido para esse fim.

8.7.1. A área técnica está autorizada a instalar somente softwares corporativos, adquiridos pelo Tribunal, com licença de uso válida.

8.7.2. A instalação de softwares livres é autorizada somente mediante análise técnica de conformidade e segurança realizada pela seção responsável pela gestão de serviços de TIC e microinformática.

8.8. É vedado à área técnica conceder aos usuários privilégios de administrador local nas estações de trabalho.

9. Da rede de dados corporativa

9.1. A conexão física de equipamentos à rede de dados corporativa, bem como a configuração e a remoção de ativos dessa rede são permitidas somente aos

técnicos que integram a área de infraestrutura tecnológica e segurança cibernética.

9.1.1. É vedada a conexão de dispositivos pessoais à rede de dados corporativa.

9.2. A área técnica responsável pela infraestrutura tecnológica e segurança cibernética deverá fazer uso de soluções tecnológicas a fim de monitorar a segurança da rede de dados corporativa.

9.2.1. Deverão ser removidos quaisquer ativos não autorizados, com imediata comunicação à Comissão de Segurança da Informação, para apuração da violação de segurança.

9.2.2. Deverão ser colocados em quarentena imediata, sem aviso prévio ao usuário, os ativos que forem identificados como potencialmente nocivos à rede de dados corporativa, seja por contaminação por vírus ou por outro tipo de anomalia.

9.2.2.1. O ativo só sairá da quarentena após minuciosa análise técnica e eliminação completa do problema.

9.2.3. Visando à garantia da segurança da rede, deverão ser bloqueados, sem aviso prévio, quaisquer usuários que forem identificados tentando transpor as medidas de segurança adotadas pela Administração.

9.2.3.1. A área técnica deverá produzir e apresentar relatório para a Comissão de Segurança da Informação, em que constem as evidências do ilícito, para apuração da violação de segurança.

9.3. A área técnica responsável pela infraestrutura tecnológica e segurança cibernética poderá fazer uso de medidas de segurança para ativos e usuários da rede de dados corporativa, a fim de elevar a segurança.

9.4. O acesso à rede de dados corporativa fornecido por meio de conexão sem fio (wifi) está sujeito aos dispositivos estabelecidos nesta norma.

10. Do uso de dispositivos de armazenamento portáteis

10.1. É vedado o uso de dispositivos de armazenamento portáveis, como pendrives e discos externos, para armazenamento de dados pessoais e informações

corporativas restritas e sigilosas. Tais informações devem ser mantidas nas unidades de rede disponibilizadas para esse fim ou em nuvem corporativa regularmente contratada.

10.2. É vedada a conexão de dispositivos de armazenamento portáteis, como pendrives e discos externos, na rede de dados corporativa.

10.2.1. Havendo necessidade de trabalho justificada, a conexão deve acontecer com supervisão da área técnica, que pode ser solicitada por meio dos canais convencionais de atendimento.

10.2.2. Excluem-se dessa categoria as mídias de resultado proveniente das urnas eletrônicas, que podem ser utilizadas regularmente na infraestrutura tecnológica.

10.2.3. Os técnicos da área de tecnologia da informação podem fazer uso desse tipo de dispositivo para cumprimento de atividades de suporte, devendo, porém, adotar todas as medidas de proteção cabíveis.

11. Do armazenamento de arquivos

11.1. Os usuários terão disponível área de armazenamento na infraestrutura de rede local, a fim de salvaguardar os arquivos relacionados ao trabalho desenvolvido.

11.1.1. As informações corporativas devem ser armazenadas nessa área.

11.1.2. A área de armazenamento do usuário terá tamanho limitado à capacidade suportada pela infraestrutura.

11.1.3. Cabe à área técnica responsável pela gestão de infraestrutura e redes a definição do tamanho da área de armazenamento e os tipos de arquivos permitidos, atentando-se para o atendimento de todos os usuários e para a segurança e o desempenho da infraestrutura tecnológica corporativa.

11.1.4. Os arquivos de usuários armazenados dentro da infraestrutura de rede, na área preestabelecida pelo setor técnico, serão automaticamente inseridos nas rotinas de backup, ficando sujeitos às regras estabelecidas em política específica de cópia de segurança e restauração de arquivos digitais.

11.2. É vedado aos usuários em relação ao armazenamento de arquivos:

11.2.1. Armazenar arquivos pessoais ou quaisquer outros arquivos não relacionados às atividades institucionais nos dispositivos corporativos ou na rede local.

11.2.2. Utilizar serviços em nuvem de caráter particular para o processamento ou armazenamento de informações de propriedade da Justiça Eleitoral, incluindo dados pessoais.

11.2.3. Manter armazenados dados pessoais controlados pelo Tribunal ou quaisquer informações corporativas relevantes ao negócio em:

11.2.3.1. equipamentos pessoais;

11.2.3.2. dispositivos de armazenamento removíveis;

11.2.3.3. discos locais das estações de trabalho corporativas e notebooks (unidades C:, D:).

11.3. Em relação às informações corporativas relevantes ao negócio ou dados pessoais controlados pelo Tribunal, que tenham sido armazenados em violação ao estabelecido no subitem 11.2:

11.3.1. Não são contemplados pela garantia prevista no subitem 11.1.4, cabendo exclusivamente ao usuário providenciar eventual cópia de segurança e eliminação.

11.3.2. Serão sumariamente excluídos, no caso de estações de trabalho corporativas e notebooks, quando o equipamento passar por processo de manutenção, de desfazimento, por ocasião de realização de procedimento de segurança ou de instalação padronizada.

11.3.3. Têm a confidencialidade, integridade, disponibilidade e autenticidade sob responsabilidade exclusiva do usuário.

11.3.4. Sujeita o usuário às penalidades estabelecidas em Lei, no caso de incidente de segurança da informação.

11.4. Os arquivos pessoais e quaisquer outros arquivos não relacionados às atividades institucionais armazenados nos servidores de rede e nos demais equipamentos corporativos serão sumariamente excluídos sempre que identificados.

11.5. O Tribunal reserva-se o direito de inspecionar, sem a necessidade de aviso prévio, os computadores e arquivos armazenados, que estejam no disco local dos computadores, nas áreas privativas ou nas áreas compartilhadas da rede, visando assegurar o cumprimento desta norma.

12. Do suporte técnico por acesso remoto

12.1. O suporte técnico por acesso remoto aos equipamentos corporativos tem por finalidade agilizar a solução dos incidentes e o cumprimento de requisições de TIC, diminuindo a necessidade de deslocamento de técnicos até o local onde está instalado o equipamento e permitindo o suporte em *homeoffice*.

12.2. O suporte técnico por acesso remoto é permitido exclusivamente aos técnicos da área de tecnologia da informação.

12.3. O suporte técnico por acesso remoto será efetuado somente por meio de software regularmente contratado para esse fim, vedado o uso de software livre.

12.3.1. Cabe à área técnica responsável pelos serviços de TIC e microinformática propor soluções de software para suporte remoto, bem como gerir e manter atualizada a solução contratada.

12.4. É obrigatória a autorização do usuário para prestação de suporte técnico por acesso remoto.

12.4.1. A autorização é exclusiva para uma sessão de suporte, devendo ser renovada cada vez que uma nova intervenção for necessária.

12.4.2. O processo de autorização deve ocorrer por meio da solução de software de suporte remoto contratada.

12.4.3. É facultado ao usuário o acompanhamento das ações técnicas durante o suporte por acesso remoto.

12.5. É vedado aos técnicos que prestam suporte por acesso remoto:

12.5.1. Acessar recursos de TIC sem finalidade específica de prestar suporte ou sem autorização do usuário.

12.5.2. Visualizar conteúdo contido no equipamento por curiosidade ou má-fé.

12.5.3. Obter cópia de conteúdos, protegidos ou não, inclusive de dados pessoais, sem a devida autorização do usuário.

12.5.4. Sabotar ou interromper intencionalmente o funcionamento de serviço ou sistema dentro de equipamento do Tribunal.

12.5.5. Copiar chaves de licença de software para uso particular.

12.5.6. Executar qualquer ação que comprometa a segurança da rede de dados corporativa ou do equipamento acessado ou, ainda, das informações nelas disponíveis.

13. Dos meios de impressão

13.1. Os recursos de impressão pertencentes a este Tribunal, disponíveis para o usuário, devem ser utilizados exclusivamente para impressão/reprodução de documentos relacionados às atividades afetas às suas funções institucionais.

13.2. São deveres do usuário no uso dos meios de impressão:

13.2.1. Retirar imediatamente da impressora ou fotocopiadora os documentos de que tenha solicitado impressão, transmissão ou cópia;

13.2.2. Não efetuar, em hipótese alguma, o reaproveitamento de páginas já impressas que contenham informações classificadas como confidenciais ou que contenham dados pessoais. Estas devem ser descartadas de forma segura;

13.2.3. Limitar as impressões e cópias à quantidade exata necessária para a tarefa determinada.

13.3. Sempre que possível, o compartilhamento seguro de documentos deve ser priorizado à impressão, evitando o uso desnecessário de insumos.

13.4. Os meios de impressão, sempre que possível, devem ser compartilhados por mais de uma unidade, visando à economicidade dos recursos e às recomendações de sustentabilidade.

13.5. O quantitativo de equipamentos destinado às Unidades será estabelecido pelo Comitê de Governança de Tecnologia da Informação e Comunicação.

14. Do uso da rede corporativa por acesso remoto

Regulado por norma específica, NSI 006.

15. Do serviço de correio eletrônico

Regulado por norma específica, NSI 010.

16. Do acesso à internet

Regulado por norma específica, NSI 001.

17. Do uso da rede sem fio corporativa

Regulado por norma específica, NSI 002.

18. Do uso de aplicativos de mensagem instantânea

Regulado por norma específica, NSI 004.

19. Das disposições finais

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

19.2. A revisão deste normativo de uso de recursos de tecnologia da informação e comunicação ocorrerá sempre que se fizer necessário ou conveniente para este Tribunal, não excedendo o período máximo de 3 (três) anos.

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

19.4. Esta norma entra em vigor na data de sua aprovação.