



Tribunal Superior Eleitoral
Secretaria de Gestão da Informação e do Conhecimento
Coordenadoria de Jurisprudência e Legislação
Seção de Legislação

RESOLUÇÃO Nº 23.644, DE 1º DE JULHO DE 2021.

Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.

O TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições e

CONSIDERANDO que a Justiça Eleitoral produz, recebe e custodia informações no exercício de suas competências constitucionais, legais e regulamentares e que essas informações devem permanecer íntegras, disponíveis e, quando for o caso, com sigilo resguardado;

CONSIDERANDO que as informações e os documentos na Justiça Eleitoral são armazenados e disponibilizados em diferentes suportes, físicos e eletrônicos, portanto, vulneráveis a incidentes, como desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto;

CONSIDERANDO a importância da adoção de boas práticas relacionadas à proteção da informação preconizadas pelas normas NBR ISO/IEC 27001:2013, NBR ISO/IEC 27002:2013, NBR ISO/IEC 27005:2019 e pelas Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário de 2012, às quais a Política de Segurança da Informação (PSI) da Justiça Eleitoral deverá estar alinhada;

CONSIDERANDO a edição do Acórdão - TCU nº 1233/2012 - Plenário, que recomenda ao Conselho Nacional de Justiça a promoção de ações para a melhoria da governança de tecnologia da informação em virtude do resultado de diagnóstico de maturidade e aderência de processos de segurança da informação;

CONSIDERANDO a Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, que estabelece diretrizes para a elaboração de Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal;

CONSIDERANDO a Resolução nº 370/2021 (<https://atos.cnj.jus.br/atos/detalhar/3706>) do Conselho Nacional de Justiça, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTICJUD);

CONSIDERANDO a Resolução nº 325/2020 (<https://atos.cnj.jus.br/atos/detalhar/3365>) do Conselho Nacional de Justiça, que institui a Estratégia Nacional do Poder Judiciário para o sexênio 2021-2026;

CONSIDERANDO a Res.-TSE nº 23.379/2012 (<https://www.tse.jus.br/legislacao/compilada/res/2012/resolucao-no-23-379-de-1-de-marco-de-2012>), que dispõe sobre o Programa de Gestão Documental no âmbito da Justiça Eleitoral;

CONSIDERANDO a Portaria TSE nº 1.013/2018 (<https://www.tse.jus.br/legislacao/compilada/prt/2018/portaria-no-1013-de-23-de-novembro-de-2018>), que institui a Política de Preservação Digital da Justiça Eleitoral;

CONSIDERANDO a Lei nº 12.527/2011 (http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm), que versa sobre o acesso à informação, especialmente quanto às normas de classificação, restrição e segurança da informação;

CONSIDERANDO a necessidade de implementar ações para garantir a adequada execução da Lei nº 13.709/2018 (http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm) (LGPD), no que tange à segurança da informação;

CONSIDERANDO o Decreto nº 9.637/2018 (http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm) , que institui a Política Nacional de Segurança da Informação no âmbito da Administração Pública Federal;

CONSIDERANDO a necessidade de orientar a condução de ações voltadas à promoção da Segurança da Informação no âmbito da Justiça Eleitoral;

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação (PSI) da Justiça Eleitoral.

CAPÍTULO I

DOS CONCEITOS E DAS DEFINIÇÕES

Art. 2º Para os efeitos desta Resolução e de suas regulamentações, aplicar-se-á o glossário de termos de segurança da informação definido em Portaria a ser expedida pelo Tribunal Superior Eleitoral.

CAPÍTULO II

DOS PRINCÍPIOS

Art. 3º Esta PSI se alinha às estratégias da Justiça Eleitoral e tem como princípio norteador a garantia da disponibilidade, integridade, confidencialidade, autenticidade, irretratabilidade e auditabilidade das informações produzidas, recebidas, armazenadas, tratadas ou transmitidas pelos órgãos da Justiça Eleitoral, no exercício de suas atividades e funções.

Art. 4º O uso adequado dos recursos de tecnologia da informação e comunicação visa garantir a continuidade da prestação jurisdicional e de serviços da Justiça Eleitoral.

§ 1º Os recursos de tecnologia da informação e comunicação, pertencentes aos órgãos da Justiça Eleitoral e que estão disponíveis para os usuários, devem ser utilizados em atividades estritamente relacionadas às funções institucionais.

§ 2º A utilização dos recursos de tecnologia da informação e comunicação é passível de monitoramento e controle por parte do Tribunal.

Art. 5º As informações produzidas por usuários, no exercício de suas atividades e funções, são patrimônio intelectual da Justiça Eleitoral, não cabendo a seus criadores qualquer forma de direito autoral.

CAPÍTULO III

DO ESCOPO

Art. 6º São objetivos da PSI da Justiça Eleitoral:

I - instituir diretrizes estratégicas, responsabilidades e competências, visando à estruturação da segurança da informação;

II - direcionar as ações necessárias à implementação e à manutenção da segurança da informação;

III - definir as ações necessárias para evitar ou mitigar os efeitos de atos acidentais ou intencionais, internos ou externos, de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos de informação e a imagem da instituição;

IV - nortear os trabalhos de conscientização e de capacitação de pessoal em segurança da informação e em proteção de dados pessoais.

Art. 7º Esta PSI 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, colaboradores e usuários externos, que fazem uso ou tenham acesso aos ativos de informação e de processamento no âmbito da Justiça Eleitoral.

Art. 8º Os destinatários desta PSI, relacionados no caput do art. 7º, são corresponsáveis pela segurança da informação, de acordo com os preceitos estabelecidos nesta Resolução, e têm como deveres:

- I - ter pleno conhecimento desta PSI e zelar por seu cumprimento;
- II - proteger as informações sigilosas e pessoais obtidas em decorrência do exercício de suas atividades;
- III - preservar o sigilo da identificação de usuário e de senhas de acessos individuais a sistemas de informação, ou outros tipos de credenciais de acesso que lhes forem atribuídos;
- IV - participar das campanhas de conscientização e dos treinamentos pertinentes aos temas segurança da informação e proteção de dados pessoais, conforme planejamento dos tribunais eleitorais;
- V - reportar qualquer falha ou incidente de segurança da informação de que tiver conhecimento, utilizando mecanismos próprios disponibilizados pelos tribunais;
- VI - utilizar os ativos sob sua responsabilidade de forma segura, em observância ao disposto nesta PSI e em eventuais normativos a ela subordinados.

CAPÍTULO IV

DAS DIRETRIZES GERAIS

Art. 9º A estrutura normativa referente à Segurança da Informação será estabelecida e organizada conforme definido a seguir:

I - Nível Estratégico: Política de Segurança da Informação da Justiça Eleitoral, constituída por esta Resolução, a qual define as diretrizes fundamentais e os princípios basilares incorporados pela instituição à sua gestão, de acordo com a visão definida pelo Planejamento Estratégico dos órgãos da Justiça Eleitoral;

II - Nível Tático: Normas Complementares sobre Segurança da Informação, que contemplam obrigações a serem seguidas de acordo com as diretrizes estabelecidas nesta PSI, a serem editadas por todos os tribunais que compõem a Justiça Eleitoral, e devem abarcar, no mínimo, os seguintes temas:

- a. Gestão de Ativos;
- b. Controle de Acesso Físico e Lógico;
- c. Gestão de Riscos de Segurança da Informação;
- d. Uso Aceitável de Recursos de TI;
- e. Geração e Restauração de Cópias de Segurança (backup);
- f. Plano de Continuidade de Serviços Essenciais de TI;
- g. Gestão de Incidentes de Segurança da Informação;
- h. Gestão de Vulnerabilidades e Padrões de Configuração Segura;
- i. Gestão e Monitoramento de Registros de Atividade (logs);
- j. Desenvolvimento Seguro de Sistemas;
- k. Uso de Recursos Criptográficos.

III - Nível Operacional: Procedimentos de Segurança da Informação que contemplam regras operacionais, roteiros técnicos, fluxos de processos, manuais com informações técnicas que instrumentalizam o disposto nas normas referenciadas no plano tático, de acordo com o disposto nas diretrizes e normas de segurança estabelecidas, permitindo sua utilização nas atividades do órgão.

§ 1º Conforme necessidade e conveniência de cada Tribunal Eleitoral, poderão ser criados normativos sobre outros temas.

§ 2º Os normativos deverão considerar as disposições contidas na família de normas ISO 27000 e na Instrução Normativa nº 01 GSI/PR/2008 - Segurança da Informação, e Comunicações e suas Normas Complementares.

CAPÍTULO V

DA ESTRUTURA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 10. Deverá ser constituída, no âmbito dos Tribunais Eleitorais, Comissão de Segurança da Informação, subordinada à Presidência do Tribunal, composta, no mínimo, por representantes da Presidência, da Corregedoria, da Diretoria-Geral, de cada Secretaria, da Assessoria de Comunicação Social ou da unidade que desempenhe essa atividade, da Unidade de Segurança e Inteligência, e dos Cartórios Eleitorais, no caso dos Tribunais Regionais.

§ 1º Os representantes indicados pelas unidades citadas no caput devem ser preferencialmente servidores da Justiça Eleitoral ou servidores públicos cedidos à Justiça Eleitoral.

§ 2º Os integrantes da Comissão de Segurança da Informação deverão assinar Termo de Sigilo em que se comprometam a não divulgar as informações de que venham a ter ciência em razão de sua participação na citada comissão para terceiros estranhos aos processos e procedimentos relativos à segurança da informação.

Art. 11. Compete à Comissão de Segurança da Informação:

I - propor melhorias a esta PSI;

II - propor normas, procedimentos, planos ou processos, nos termos do art. 9º, visando à operacionalização desta PSI;

III - promover a divulgação desta PSI, de outros normativos e de ações para disseminar a cultura em segurança da informação, no âmbito do Tribunal Eleitoral;

IV - propor estratégias para a implantação desta PSI;

V - propor ações visando à fiscalização da aplicação das normas e da política de segurança da informação;

VI - propor recursos necessários à implementação das ações de segurança da informação;

VII - propor a realização de análise de riscos e o mapeamento de vulnerabilidades nos ativos;

VIII - propor a abertura de sindicância para investigar e avaliar os danos decorrentes de quebra de segurança da informação;

IX - propor o modelo de implementação da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR), de acordo com a norma vigente;

X - propor a constituição de grupos de trabalho para tratar de temas sobre segurança da informação;

XI - representar o Tribunal Eleitoral nos contatos com entidades externas necessárias ao tratamento de incidentes de segurança da informação, à exceção dos casos atribuídos à ETIR;

XII - responder pela segurança da informação.

Art. 12. Caberá, especificamente, à Comissão de Segurança da Informação do Tribunal Superior Eleitoral:

I - apresentar à alta administração do TSE proposta de revisão da PSI da Justiça Eleitoral, no máximo, a cada três anos, de modo a atualizá-la, em razão de novos requisitos corporativos de segurança;

II - avaliar e referendar proposições encaminhadas pelas Comissões de Segurança da Informação dos Tribunais Regionais Eleitorais para melhoria desta PSI;

III - propor modelos de normas, procedimentos, planos e processos, visando auxiliar a operacionalização desta política no âmbito dos Tribunais Eleitorais;

IV - promover, em âmbito nacional, a divulgação desta PSI e de ações para disseminar a cultura em segurança da informação.

Art. 13. Deverá ser nomeado um Gestor de Segurança da Informação, no âmbito de cada Tribunal Eleitoral, com as seguintes responsabilidades:

I - propor normas relativas à segurança da informação à Comissão de Segurança da Informação;

II - propor iniciativas para aumentar o nível da segurança da informação à Comissão de Segurança da Informação, com base, inclusive, nos registros armazenados pela ETIR;

III - propor o uso de novas tecnologias na área de segurança da informação;

IV - implantar, em conjunto com as demais áreas, normas, procedimentos, planos ou processos elaborados pela Comissão de Segurança da Informação;

V - acompanhar os processos de Gestão de Riscos em Segurança da Informação e de Gestão de Vulnerabilidades;

VI - definir e acompanhar indicadores de aderência à PSI;

VII - analisar criticamente o andamento dos processos de segurança da informação e apresentar suas considerações à Comissão de Segurança da Informação.

Parágrafo único. O Gestor de Segurança da Informação deverá ser servidor que detenha amplo conhecimento dos processos de negócio do Tribunal e do tema objeto desta Resolução.

Art. 14. Deverá ser instituída Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética - ETIR, conforme modelo proposto pela Comissão de Segurança da Informação e aprovado pelo Diretor-Geral da Secretaria do Tribunal, com a responsabilidade de receber, analisar, classificar, tratar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores, além de armazenar registros para formação de séries históricas, como subsídio estatístico, e para fins de auditoria.

§ 1º Caberá à ETIR elaborar o Processo de Tratamento e Resposta a Incidentes em Redes Computacionais no âmbito do Tribunal Eleitoral.

§ 2º Poderá a ETIR comunicar a ocorrência de incidentes em redes de computadores aos Centros de Tratamento de Incidentes ligados a entidades de governo, ao Centro de Tratamento de Incidentes em Redes Computacionais do Poder Judiciário, tão logo esteja implantado, e ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br, sempre que a cooperação seja necessária para prover uma melhor resposta ao incidente.

§ 3º Caberá à ETIR de cada Tribunal a comunicação com as equipes congêneres de outros Tribunais Eleitorais para o tratamento de incidentes de segurança comuns aos tribunais envolvidos.

§ 4º Caso a ETIR não esteja constituída ou não esteja em operação, as atribuições definidas neste artigo caberão à Secretaria de Tecnologia da Informação.

CAPÍTULO VI

DO PROCESSO DE TRATAMENTO DA INFORMAÇÃO

Art. 15. O tratamento da informação deve abranger as políticas, os processos, as práticas e os instrumentos utilizados pela Justiça Eleitoral para lidar com a informação ao longo de cada fase do seu ciclo de vida, contemplando o conjunto de ações referentes às fases de produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Art. 16. As informações produzidas ou custodiadas pela Justiça Eleitoral devem ser tratadas em função do seu grau de confidencialidade, criticidade e temporalidade, garantindo-se a sua integridade, autenticidade, disponibilidade e a cadeia de custódia dos documentos.

§ 1º Serão protegidas quanto à confidencialidade as informações classificadas e as que possuem sigilo em decorrência de previsão legal, nos termos da Lei de Acesso à Informação e de sua regulamentação em cada Tribunal Eleitoral.

§ 2º Serão protegidas quanto à integridade, autenticidade e disponibilidade todas as informações, adotando-se medidas de proteção de acordo com a criticidade atribuída a cada informação.

§ 3º Os direitos de acesso aos sistemas de informação e às bases de dados da Justiça Eleitoral deverão ser concedidos aos usuários em estrita observância à efetiva necessidade de tal acesso para a execução de suas atividades e funções em cada Tribunal, observadas, no que couber, as disposições da Lei de Acesso à Informação.

§ 4º A regulamentação das informações classificadas em cada Tribunal deverá ser proposta pelo Núcleo de Credenciamento da Informação, Comissão de Segurança da Informação ou unidade a quem tal responsabilidade tenha sido atribuída, em conjunto com a unidade ou comissão responsável pela gestão da informação no Tribunal.

§ 5º As informações ostensivas de interesse público deverão ser disponibilizadas independentemente de solicitações, observadas a Política e Planos de Dados Abertos ou determinações semelhantes em cada Tribunal.

Art. 17. Toda informação classificada, em qualquer grau de sigilo, produzida, armazenada ou transmitida pelo Tribunal, em parte ou totalmente, por qualquer meio eletrônico, deverá ser protegida com recurso criptográfico.

Parágrafo único. A falta de proteção criptográfica poderá ocorrer quando justificada e aprovada pela unidade gestora de riscos, ou pela Comissão de Segurança da Informação, ou quando prevista em normativo específico.

CAPÍTULO VII

DAS COMPETÊNCIAS DAS UNIDADES

Art. 18. Compete à Presidência:

I - apoiar a aplicação das ações estabelecidas nesta PSI;

II - nomear ou delegar ao Diretor-Geral da Secretaria a nomeação:

a) do Gestor da Comissão de Segurança da Informação, nos termos do art. 10;

b) do Gestor de Segurança da Informação e seu substituto, nos termos do art. 13, parágrafo único;

c) de integrantes da ETIR, nos termos do art. 14.

Art. 19. Compete ao Diretor-Geral da Secretaria do Tribunal:

I - aprovar normas, procedimentos, planos ou processos que lhe forem submetidos pela Comissão de Segurança da Informação;

II - submeter à Presidência as propostas que extrapolem sua alçada decisória;

III - apoiar a aplicação das ações estabelecidas nesta PSI;

IV - viabilizar financeiramente as ações de implantação desta PSI, inclusive a exequibilidade do Plano de Continuidade de Serviços Essenciais de TI, abrangendo manutenção, treinamento e testes periódicos.

Art. 20. Compete à Secretaria de Tecnologia da Informação:

I - apoiar a implementação desta PSI;

II - prover os ativos de processamento necessários ao cumprimento desta PSI;

III - garantir que os níveis de acesso lógico concedidos aos usuários, de acordo com os direitos de acesso definidos pelos gestores dos sistemas de informação, estejam adequados aos propósitos do negócio e condizentes com as normas vigentes de segurança da informação;

IV - disponibilizar e gerenciar a infraestrutura necessária aos processos de trabalho da ETIR;

V - executar as orientações e os procedimentos estabelecidos pela Comissão de Segurança da Informação.

Art. 21. As demais unidades organizacionais de cada Tribunal deverão apoiar, observadas suas atribuições regimentais, as estruturas organizacionais responsáveis pela Gestão da Segurança da Informação, conforme definições constantes no Capítulo V.

CAPÍTULO VIII

DAS DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Art. 22. A próxima revisão desta Política de Segurança da Informação deverá considerar, entre outros, os seguintes temas:

I - utilização de computação em nuvem;

II - aspectos de segurança da informação sobre o trabalho remoto;

III - adoção de novos sistemas ou soluções de TIC, considerando os aspectos relativos à segurança da informação.

Art. 23. Os casos omissos desta PSI serão resolvidos pelas Comissões de Segurança da Informação dos Tribunais Eleitorais.

Art. 24. Esta PSI é obrigatória a todos os Tribunais Eleitorais, os quais terão até 31 de dezembro de 2021 para se adaptarem às regras previstas nesta Resolução.

Art. 25. Esta PSI e demais normas, procedimentos, planos ou processos deverão ser publicados na intranet de cada Tribunal pela respectiva Comissão de Segurança da Informação, caso não afetem a segurança das operações do Tribunal.

Parágrafo único. As diretrizes normativas de que trata o caput deste artigo também devem ser divulgadas a todos os citados no art. 7º no momento da sua posse/admissão, além de a outras pessoas que se encontrem a serviço ou em visita às unidades da Justiça Eleitoral, autorizadas a utilizar temporariamente os recursos de tecnologia da informação e comunicação da instituição.

Art. 26. O descumprimento desta PSI será objeto de apuração pela unidade competente do Tribunal, mediante sindicância ou processo administrativo disciplinar, e pode acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 27. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo Tribunal deverão observar, no que couber, o constante desta PSI.

Art. 28. Deverá ser incluída no escopo do Plano Anual de Auditoria e Conformidade a análise do correto cumprimento desta PSI, de seus regulamentos e demais normativos de segurança vigentes, conforme planejamento estabelecido pela Unidade de Auditoria Interna, abrangendo uma ou mais normas, procedimentos, planos ou processos estabelecidos.

Art. 29. A PSI e a Política Geral de Privacidade e Proteção de Dados Pessoais da Justiça Eleitoral* são complementares, devendo ser interpretadas em conjunto.

Art. 30. Esta Resolução entra em vigor na data de sua publicação, revogada a Res.-TSE nº 23.501 (<https://www.tse.jus.br/legislacao/compilada/res/2016/resolucao-no-23-501-de-19-de-dezembro-2016>) , de 19 de dezembro de 2016.

Brasília, 1º de julho de 2021.

MINISTRO LUÍS ROBERTO BARROSO - RELATOR

Este texto não substitui o publicado no DJE-TSE, nº 129, de 8.7.2021, p. 12-18.

(<https://sintse.tse.jus.br/documentos/2021/Jul/8/diario-da-justica-eletronico-tse/resolucao-no-23-644-de-1o-de-julho-de-2021-dispoe-sobre-a-politica-de-seguranca-da-informacao-psi-no>)

*Vide Resolução nº 23.650/2021 (<https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-650-de-9-de-setembro-de-2021>), que Institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral.