Juiz Federal

RESOLUÇÕES

RESOLUÇÃO N.º 110, DE 10 DE AGOSTO DE 2023

INSTITUI A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) NO ÂMBITO DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE.

O TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a Resolução nº 370, de 28 de janeiro de 2021, do Conselho Nacional de Justiça, que, em seu art. 21, inciso II, determina que cada órgão deverá constituir e manter estruturas organizacionais adequadas e compatíveis de acordo com a demanda de TIC, considerando, entre outros, o macroprocesso de Segurança da Informação e Proteção de Dados;

CONSIDERANDO a Resolução nº 396, de 7 de junho de 2021, do Conselho Nacional de Justiça, que, em seu art. 19º, inciso II, determina que cada órgão deverá elaborar a Política de Segurança da Informação e normas internas correlatas ao tema, observadas as normas de segurança da informação editadas pelo CNJ;

CONSIDERANDO as Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário de 2012, elaboradas pelo Conselho Nacional de Justiça;

CONSIDERANDO a Resolução nº 23.644, de 1º de julho de 2021, do Tribunal Superior Eleitoral, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a Resolução nº 23.650, de 9 de setembro de 2021, do Tribunal Superior Eleitoral, que institui a Política de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral;

CONSIDERANDO a necessidade de implementar ações para garantir a adequada execução da Lei nº 13.709/2018 (LGPD), no que tange à segurança da informação;

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 27005:2011;

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 Resolução nº 23.379, de 1º de março de 2012, do Tribunal Superior Eleitoral, que dispõe sobre o Programa de Gestão Documental no âmbito da Justiça Eleitoral;

CONSIDERANDO a Lei nº 12.527, de 18 de novembro de 2011, que versa sobre o acesso à informação, previsto na Constituição Federal, e a Resolução TRE/RN nº 15/2016, que regulamenta a sua aplicação, no âmbito do TRE/RN;

CONSIDERANDO a Resolução TRE/RN nº 22/2016, que dispõe sobre as diretrizes para a implantação do Programa de Gestão Documental (PGD), no âmbito da Justiça Eleitoral do Rio Grande do Norte;

CONSIDERANDO a necessidade de implantação da estrutura normativa, que reflita as diretrizes, deveres e responsabilidades referentes à Segurança da Informação;

CONSIDERANDO que a geração, aquisição, absorção e manutenção das informações no exercício de suas competências devem permanecer íntegras, disponíveis e, quando aplicável, com o sigilo resguardado;

CONSIDERANDO que a gestão da informação deve nortear todos os processos de trabalho e unidades do Tribunal e ser impulsionada e respaldada por uma política corporativa de segurança da informação;
CONSIDERANDO o que consta nos autos do PAE nº 6330/2023 (PJE - PA nº 0600317-79.2023.6.20.0000);
RESOLVE:
Art. 1º Fica regulamentada, nos termos desta Resolução, a Política de Segurança da Informação (PSI), no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte.
Parágrafo único. Por Política de Segurança da Informação compreende-se o documento que declara o comprometimento da Administração com a gestão segura das suas informações, orienta e vincula todos os usuários para o adequado manuseio, armazenamento, transporte e descarte das informações pelos usuários internos e externos, por meio da adoção de procedimentos e mecanismos, que visam a eliminação ou redução da ocorrência de modificações não autorizadas, bem como garantam a disponibilidade de recursos e sistemas críticos para a continuidade dos negócios do TRE-RN, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores praticas de Segurança da Informação e Comunicação.
Capítulo I
DAS DEFINIÇÕES E CONCEITOS TÉCNICOS
Art. 2º Para efeitos desta Resolução e de suas regulamentações, aplicam-se as seguintes definições:
I - ameaça: causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;
II - atividades precípuas: conjunto de procedimentos e tarefas que utilizam recursos tecnológicos, humanos e materiais, inerentes à atividade-fim da Justiça Eleitoral;
III - atividades críticas: atividades precípuas da Justiça Eleitoral cuja interrupção ocasiona severos transtornos, como, por exemplo, perda de prazos administrativos e judiciais, dano à imagem institucional, prejuízo ao Erário, entre outros;
IV - ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;
V - ativo de informação: patrimônio composto por todos os dados e informações gerados, adquiridos, utilizados ou armazenados pela Justiça Eleitoral;
VI - ativo de processamento: patrimônio composto por todos os elementos de hardware, software e infraestrutura de comunicação necessários à execução das atividades precípuas da Justiça Eleitoral;
VII - ciclo de vida da informação: ciclo formado pelas fases de produção, recepção, organização, uso, disseminação e destinação;
VIII - cifração: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro por outros ininteligíveis a pessoas não autorizadas a conhecê-los;
IX - colaboradores: Pessoa física ou jurídica que contribui para os serviços eleitorais, voluntariamente ou por imposição legal, sem remuneração;
X - continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;
XI - criticidade: princípio de segurança que define a importância da informação para a continuidade do negócio;

XII - custodiante: responsável pelo processamento ou armazenamento da informação nas tarefas de rotina por delegação do gestor da informação;
XIII - dados: representação de fatos, conceitos e instruções, por meio de sinais de uma maneira formalizada, possível de ser transmitida ou processada pelo homem ou por máquinas;
XIV - decifração: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;
XV - diretriz: descrição que orienta o que deve ser feito e como, para se alcançarem objetivos estabelecidos nas políticas;
XVI - disponibilidade: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada;
XVII - documento: unidade de registro de informações, qualquer que seja o formato ou o suporte;
XVIII - gestão de riscos: atividades coordenadas para dirigir e controlar uma organização, no que se refere aos riscos. Normalmente inclui a avaliação, o tratamento, a aceitação e a comunicação do risco;
XIX - gestão de segurança da informação: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade de negócios, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando à tecnologia da informação;
XX - incidente de segurança em redes computacionais: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
XXI - incidente em segurança da informação: qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações do negócio ou ameaçar a segurança da informação;
XXII - informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;
XXIII - plano de continuidade de serviços essenciais de TI: conjunto de medidas de prevenção e recuperação de ativos, com o objetivo de manter a disponibilidade de serviços e atividades do negócio, protegendo assim os processos críticos contra impactos causados por falhas ou desastres e, no caso de perdas, prover a recuperação dos ativos envolvidos e restabelecer o funcionamento normal da organização no menor tempo possível;
XXIV - proprietário da informação: pessoa ou setor que produz a informação, capaz de estimar em que nível de criticidade ela se enquadra;
XXV - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;
XXVI - recurso: além da própria informação, é todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;
XXVII - recurso criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;
XXVIII - rede de computadores: rede formada por um conjunto de máquinas eletrônicas com processadores capazes de trocar informações e partilhar recursos, interligados por um subsistema de comunicação, ou seja, existência de dois ou mais computadores, e outros dispositivos interligados entre si de modo a poder compartilhar recursos físicos e lógicos, sendo que estes podem ser do tipo dados, impressoras, mensagens (e-mails), entre outros;
XXIX - risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;

XXX - segurança da informação: abrange aspectos físicos, tecnológicos e humanos da organização e orienta-se pelos princípios da autenticidade, da confidencialidade, da integridade, da disponibilidade e da irretratabilidade da informação, entre outras propriedades;
XXXI - tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;
XXXII - usuário externo: qualquer pessoa física ou jurídica a quem tenha sido concedido acesso aos serviços da Justiça Eleitoral e não se inclua no conceito de usuário interno;
XXXIII - usuário interno: qualquer pessoa física que faça uso de informações e exerça atividade na Justiça Eleitoral do Rio de Grande do Norte, ainda que temporariamente, com ou sem remuneração;
XXXIV - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.
Capítulo II
DOS PRINCÍPIOS
Art. 3º Esta PSI alinha-se às estratégias e à Política de Segurança da Informação da Justiça Eleitoral, instituída por meio da Resolução TSE n.º 23.644, de 01º de julho de 2021, além da Resolução CNJ n.º 370/2021 (ENTIC-JUD).
Art. 4º As ações relacionadas com a Segurança da Informação no TRE-RN são norteadas pelos seguintes princípios, assim definidos:
I - confidencialidade: propriedade da informação que garante que ela não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem a devida autorização;
II - integridade: garantia que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
III - disponibilidade: garantia de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade autorizada;
IV - autenticidade: garantia de que a informação foi produzida, enviada, modificada ou destruída dentro dos preceitos legais e normativos, por pessoa física, ou por sistema, órgão ou entidade autorizada;
V - irretratabilidade (ou não-repúdio): garantia de que a autoria da informação não pode ser negada em uma alteração anteriormente feita, por pessoa física, ou por sistema, órgão ou entidade autorizada;
VI - auditabilidade: capacidade do Sistema de Gestão de Segurança da Informação de se sujeitar à avaliação de conformidade e desempenho dos controles internos estabelecidos para mitigar riscos. É a qualidade de algo que se pode analisar de maneira metódica e a capacidade de aferir práticas com características explicativas e informações rastreáveis, de modo a ensejar uma análise crítica das informações fornecidas.
Capítulo III
DO ESCOPO
Art. 5º São objetivos desta PSI:
I - instituir diretrizes estratégicas, responsabilidades e competências visando à estruturação das normas de segurança da informação no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte;
II - promover e viabilizar ações necessárias à implementação e à manutenção da segurança da informação;
III - prevenir, mitigar e/ou combater atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos de informação e a imagem da instituição;

IV - promover a conscientização e a capacitação dos usuários em segurança da informação.

Art. 6º As disposições desta Política de Segurança da Informação, normas e procedimentos relacionados aplicam-se a todos os magistrados, membros do Ministério Público Eleitoral, servidores efetivos, cedidos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço, colaboradores, residentes e usuários externos que fazem uso dos ativos de informação e de processamento, no âmbito da Justiça Eleitoral do Rio Grande do Norte.

Parágrafo único. Os destinatários desta PSI, relacionados no *caput*, 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.

Art. 7º O uso adequado dos recursos de tecnologia da informação e comunicação visa garantir a continuidade da prestação jurisdicional deste Tribunal.

§1º Os recursos de tecnologia da informação e comunicação, pertencentes ao Tribunal Regional Eleitoral do Rio Grande do Norte e que estão disponíveis para os usuários relacionados no art. 6º 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.

§3º Não será permitido o uso de *pendrives* ou de unidades externas de armazenamento em estações deste Tribunal, salvo em situações previstas e necessárias para o negócio.

Art. 8º As informações geradas no âmbito deste Tribunal são de sua propriedade, independente da forma de apresentação ou armazenamento. Assim, essas informações devem ser adequadamente protegidas e utilizadas exclusivamente para os fins relacionados às atividades desenvolvidas neste Tribunal.

Parágrafo único. O acesso a informações produzidas ou custodiadas pela Justiça Eleitoral que não sejam de domínio público, quando autorizado, será condicionado ao aceite a termo de sigilo e responsabilidade.

Capítulo IV

DA ESTRUTURA NORMATIVA

Art. 9º A estrutura normativa da segurança da informação, no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte, será estabelecido e organizado conforme demonstrado a seguir:

I - Nível Estratégico: Política de Segurança da Informação, constituída por esta Resolução, a qual define as diretrizes fundamentais e princípios basilares incorporados pela instituição à sua gestão, de acordo com a visão definida pelo Planejamento Estratégico da Instituição e segundo as orientações da PSI 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 e devem abarcar, no mínimo:

a) Gestão de Ativos;

b) Controle de Acesso Físico e Lógico;

c) Gestão de Riscos de Segurança da Informação;

d) Uso Aceitável de Recurso 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 Registro de Atividades (logs);

j) Desenvolvimento de Sistemas Seguros;

k) Uso de Recursos Criptográficos;

l) Implantação e Gestão de Sistemas com foco na Segurança da Informação;

m) Configuração Segura de Ambientes no âmbito do TRE.

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.

Art. 10. Os documentos integrantes da estrutura normativa da Segurança da Informação deverão ser revisados, com vistas à sua adequação aos preceitos da presente Política, conforme os critérios a seguir:

I - Em se tratando de documento de Nível Estratégico, pelo Pleno do TRE-RN, no prazo máximo de três anos;

II - Em se tratando de documento de Nível Tático, pela Presidência do TRE-RN, no prazo máximo de dois anos;

III - Em se tratando de documento de Nível Operacional, pela Diretoria-Geral do TRE-RN, no prazo máximo de um ano.

Art. 11. Esta Resolução, normas complementares, procedimentos e normas técnicas integrantes desta estrutura normativa devem ser divulgadas a todos os magistrados, servidores, estagiários, residentes e prestadores de serviço quando da sua posse/admissão, bem como, através dos meios oficiais de divulgação interna da instituição e, também, publicadas na Intranet institucional, exceto os documentos sigilosos, de maneira que seu conteúdo possa ser consultado a qualquer momento.

Capítulo V

DA ESTRUTURA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Seção I

Da Comissão Permanente de Segurança da Informação

Art. 12. A Comissão Permanente de Segurança da Informação da Justiça Eleitoral do Rio Grande do Norte (CPSI), subordinada à Presidência do Tribunal, será composta por representantes da Presidência, Corregedoria Regional Eleitoral, Diretoria-Geral, da Assessoria de Comunicação Social e Cerimonial, Secretaria Judiciária, Secretaria de Administração, Orçamento e Finanças, Secretaria de Gestão de Pessoas, Secretaria de Tecnologia da Informação e Eleições, Núcleo de Segurança da Presidência e Representantes dos Cartórios Eleitorais, tem como competências:

I - propor melhorias à Política de Segurança da Informação da Justiça Eleitoral e a esta própria Política;

II - propor normas, procedimentos, planos e/ou processos, nos termos do art. 9º, visando à operacionalização desta PSI;
III - promover a divulgação desta PSI e normativos, bem como ações para disseminar a cultura em segurança da informação, no âmbito deste Tribunal;
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 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 - responder pela segurança da informação;
XII - analisar periodicamente os incidentes de segurança da informação e ações corretivas correlatas, comunicadas pela ETIR;
XIII - promover processos de gerenciamento de riscos, bem como a elaboração e aprovação dos planos de continuidade de negócios.
§1º A CPSI poderá requisitar temporariamente servidores das unidades do Tribunal para colaborar com as atividades da Comissão.
§2º Sempre que necessário, a CPSI poderá solicitar aos titulares das unidades informações pertinentes à segurança da informação.
§3º O ato de designação da Comissão de Segurança da Informação indicará o seu presidente, o substituto eventual desse e o secretário.
Seção II
Da Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais
Art. 13. A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) estará vinculada à Secretaria de Tecnologia da Informação e Eleições e terá como responsabilidade receber, analisar, classificar, tratar e responder às notificações e atividades relacionadas a incidentes de segurança cibernética, 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 de Segurança Cibernética no âmbito do Tribunal Eleitoral.
§ 2º 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.
Seção III
Do Gestor de Segurança da Informação
Art. 14. O Gestor de Segurança da Informação atuará 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 Permanente 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 e/ou processos elaborados pela Comissão Permanente de Segurança da Informação.
V - acompanhar os processos de Gestão de Riscos em Segurança da Informação e de Gestão de Vulnerabilidades;

§ 1º O Gestor de Segurança da Informação deverá ser servidor que detenha amplo conhecimento dos processos de negócio do Tribunal e do tema em foco.
§ 2º Fica assegurado ao Gestor de Segurança da Informação, a qualquer tempo, o poder cautelar de suspender, temporariamente, o serviço ou o acesso de usuário a ativo da informação da Justiça Eleitoral do Rio Grande do Norte, quando houver indícios de incidente de segurança da informação, devendo o fato ser comunicado imediatamente à Comissão Permanente de Segurança da Informação, que levará subsídios à Diretoria-Geral para decisão definitiva.
§ 3º Fica assegurado ao Gestor de Segurança da Informação, a qualquer tempo, o poder cautelar de suspender, temporariamente, o serviço ou o acesso de usuário a ativo da informação da Justiça Eleitoral do Rio de Janeiro, quando houver indícios de riscos à segurança da informação, devendo o fato ser comunicado imediatamente à Diretoria-Geral para decisão definitiva.
§ 4º Sempre que necessário, o Gestor de Segurança da Informação poderá solicitar aos titulares das unidades informações pertinentes à segurança 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 do TRE-RN:

I - apoiar a aplicação das ações estabelecidas nesta PSI, por meio de sua Assessoria de Integração;
II - nomear ou delegar ao Diretor-Geral da Secretaria a nomeação:
a) dos componentes da Comissão Permanente de Segurança da Informação;
b) do Gestor de Segurança da Informação e seu substituto;
c) de integrantes da ETIR.
Art. 19. Compete à Vice-Presidência e Corregedoria Regional Eleitoral empreender medidas e expedir normas para adequar as práticas cartorárias a esta PSI ou propô-las à Corregedoria-Geral Eleitoral, nos casos em que for competência desta.
Art. 20. Compete à Diretoria-Geral da Secretaria do Tribunal:
I - aprovar normas, procedimentos, planos e/ou processos que lhe forem submetidos pela Comissão Permanente 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 do Tribunal, abrangendo sua manutenção, treinamento e testes periódicos.
Art. 21. Compete à Secretaria de Tecnologia da Informação e Eleições, na sua área de atuação:
I - prover o apoio necessário à implementação e compreensão da PSI;
II - prover os ativos de processamento necessários ao cumprimento desta PSI;
III - garantir que os níveis de acesso lógico concedidos aos usuários 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 - subsidiar a Comissão Permanente de Segurança da Informação com o conhecimento de cunho tecnológico, aplicado à execução desta Política.
Art. 22. Compete à Secretaria de Administração, Orçamento e Finanças:
I - assegurar que os empregados das empresas prestadoras de serviço contratadas conheçam suas atribuições e responsabilidades em relação à segurança da informação;
II - adotar as medidas necessárias por ocasião do desligamento de empregados das empresas prestadoras de serviço contratadas e comunicar às demais unidades do Tribunal, com vistas à pertinente remoção dos acessos às informações da Justiça Eleitoral.
Art. 23. Compete à Secretaria de Gestão de Pessoas:
I - apoiar a Comissão de Segurança da Informação na missão de assegurar que os magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo e estagiários conheçam suas atribuições e responsabilidades em relação à segurança da informação;
II - adotar as medidas necessárias por ocasião do desligamento de pessoal e comunicar ao Gabinete e Apoio a Planejamento e Gestão da Secretaria de Tecnologia da Informação e Eleições, com vistas à pertinente remoção dos acessos às informações da Justiça Eleitoral;
III - promover a capacitação dos servidores que integram a estrutura de gestão da segurança da informação, no que for pertinente;
Art. 24. Compete à Secretaria Judiciária regulamentar e coordenar o processo de classificação da informação no âmbito do Tribunal.
Art. 25. Compete ao Núcleo de Segurança Institucional e Inteligência:
I - implantar controles nos ambientes físicos, visando prevenir danos, furtos, roubos, interferência e acesso não autorizado às instalações e ao patrimônio da Justiça Eleitoral; e
II - implantar controles e proteção contra ameaças externas ou decorrentes do meio ambiente, como incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e desastres naturais ou causados pelo homem;

Art. 26. Compete à Assessoria de Comunicação Social e Cerimonial em conjunto com a Comissão Permanente de Segurança da Informação:
I - promover campanhas de conscientização sobre a importância da segurança da informação;
II - divulgar esta PSI.
Art. 27. Compete à unidade de Auditoria Interna incluir no escopo do Plano Anual de Auditoria e Conformidade a análise do cumprimento desta PSI, seus regulamentos e demais normativos de segurança vigentes.
Art. 28. Compete ao Juízo Eleitoral:
I - apoiar a Comissão de Segurança da Informação na missão de assegurar que os magistrados, servidores efetivos e requisitados, estagiários, prestadores de serviço e colaboradores conheçam suas atribuições e responsabilidades em relação à segurança da informação;
II - executar as orientações técnicas e os procedimentos estabelecidos pela Comissão Permanente de Segurança da Informação.
Art. 29. Compete aos titulares de todas as unidades do Tribunal, no âmbito das suas áreas de atuação:
I - auxiliar o Gestor da Segurança da Informação no estabelecimento de regras, no empreendimento das ações referentes à organização, à coordenação, ao controle e à supervisão dos assuntos relacionados à segurança da informação;
II - promover o cumprimento das normas e procedimentos atinentes à PSI;
III - propor ao Gestor de Segurança da Informação a adoção de medidas preventivas ou corretivas relacionadas à segurança da informação, bem como a criação, alteração ou adequação das normas desta PSI para resguardar a segurança da informação;
IV - incluir cláusulas nos contratos de prestação de serviços que especifiquem as sanções a que estão sujeitos os empregados das empresas contratadas, em caso de tentativa ou efetivo acesso não autorizado, uso indevido das informações e violação das normas desta PSI;
V - promover o adequado manuseio e armazenamento de documentos, processos e demais ativos de informação, inclusive os classificados como sigilosos em locais específicos;
VI - propor projetos e providências com o objetivo de viabilizar o cumprimento desta PSI;
VII - propor ao Gestor da Segurança da Informação procedimentos visando à regulamentação e operacionalização das diretrizes e normas de segurança apresentadas por esta PSI; e
VIII - executar as orientações técnicas e os procedimentos estabelecidos pela Comissão Permanente de Segurança da Informação.
Art. 30. Compete aos usuários:
I - responder por toda atividade executada com o uso de sua identificação;
II - ter pleno conhecimento e seguir esta PSI;
III - reportar tempestivamente ao Gestor de Segurança da Informação ou à CPSI quaisquer falhas ou indícios de falhas de segurança de que tenha conhecimento ou suspeita;
IV - proteger as informações sigilosas e pessoais obtidas em decorrência do exercício de suas atividades;
V - executar as orientações técnicas e os procedimentos estabelecidos pela Comissão de Segurança da Informação;
VI - gerenciar os ativos sob sua responsabilidade;
VII - observar o adequado manuseio e armazenamento de documentos e processos.
Parágrafo único. Qualquer usuário poderá encaminhar ao Gestor de Segurança da Informação ou à CPSI, para apreciação, sugestão para melhoria da Política, Normas e Procedimentos de Segurança da Informação.
CAPÍTULO VIII
DAS VIOLAÇÕES E SANÇÕES

Art. 31. São consideradas violações à política, às normas ou aos procedimentos de Segurança da Informação as seguintes situações, não se limitando às mesmas:

I - quaisquer ações ou situações que possam expor a instituição à perda financeira e/ou de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação e comunicação;

II - utilização indevida de dados institucionais e divulgação não autorizada de informações, sem a permissão expressa do proprietário da informação;

III - uso de dados, informações ou recursos de TI para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação da instituição;

IV - a não comunicação imediata ao Gestor de Segurança da Informação de quaisquer descumprimentos da política, de normas ou de procedimentos de Segurança da Informação, que porventura um usuário venha a tomar conhecimento.

Art. 32. O descumprimento desta PSI será objeto de apuração pela unidade competente do Tribunal por meio da implantação de sindicância ou processo administrativo disciplinar podendo acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Capítulo IX

DAS DISPOSIÇÕES FINAIS

Art. 33. Esta norma e os instrumentos normativos gerados a partir dela deverão ser revisados sempre que se fizerem necessários.

Art. 34. Esta PSI e demais normas, procedimentos, planos e/ou processos deverão ser publicados na Intranet do Tribunal pela Comissão Permanente de Segurança da Informação, garantindo seu amplo conhecimento para adequado usufruto dos benefícios e assunção das responsabilidades sobre os ativos de informação deste Tribunal.

Art. 35. As normas internas do TRE-RN que tratam de assuntos relacionados à segurança da informação deverão ser revisadas, com vistas à sua adequação aos preceitos da presente Política, no prazo de 12 (doze) meses, contados a partir da data da publicação desta Resolução.

Art. 36. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres, celebrados pelo Tribunal, devem observar, no que couber, as diretrizes, normas e procedimentos estabelecidos nesta PSI.

Art. 37. Os casos omissos desta PSI serão resolvidos pela Comissão Permanente de Segurança da Informação, juntamente com o Gestor de Segurança da Informação.

Art. 38. Fica revogada a Resolução TRE/RN n.º 20, de 11 de setembro de 2019.

Art. 39. Esta Resolução entra em vigor na data de sua publicação.

Sala das Sessões, Natal (RN), 10 de agosto de 2023.

Desembargador Cornélio Alves

Presidente

Desembargador Expedito Ferreira

Vice-Presidente e Corregedor Regional Eleitoral

Juiz Fábio Luiz de Oliveira Bezerra

Juíza Maria Neíze de Andrade Fernandes

Juíza Ticiana Maria Delgado Nobre

Juiz Fernando de Araújo Jales Costa

Juiz Daniel Cabral Mariz Maia

Gilberto Barroso de Carvalho Júnior

Procurador Regional Eleitoral