



TRIBUNAL REGIONAL ELEITORAL DO CEARÁ

RESOLUÇÃO N.º 920

(24 DE OUTUBRO DE 2022)

INSTITUI A POLÍTICA DE SEGURANÇA DA
INFORMAÇÃO - PSI NO ÂMBITO DA
JUSTIÇA ELEITORAL DO CEARÁ.

O **TRIBUNAL REGIONAL ELEITORAL DO CEARÁ**, no uso de suas atribuições conferida pelo art. 20, inciso IX, de seu Regimento Interno, por sua composição plena, e

CONSIDERANDO a Lei nº 12.527, de 18 de novembro de 2011, que versa sobre o acesso à informação previsto na Constituição Federal;

CONSIDERANDO a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

CONSIDERANDO a Lei nº 12.737, de 20 de novembro de 2012, que dispõe sobre a tipificação criminal de delitos informáticos;

CONSIDERANDO a Resolução nº 370, de 28 de janeiro de 2021, do Conselho Nacional de Justiça, que, em seu art. 21, determina que cada órgão deverá elaborar e aplicar política, gestão e processo de segurança da informação a serem desenvolvidos;

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 que o Tribunal produz e custodia informações no exercício de suas competências e que o sigilo dessas informações deve ser preservado;

CONSIDERANDO a Resolução nº 396, de 7 de junho de 2021, do Conselho Nacional de Justiça, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ); e

CONSIDERANDO a necessidade de implementar neste Regional a Política de Segurança da Informação - PSI, visando preservar a confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade e conformidade dos ativos de informação da Justiça Eleitoral do Ceará, sob o condão dos princípios que regem a Administração Pública,

RESOLVE:

CAPÍTULO I DAS DISPOSIÇÕES GERAIS

Art. 1º Instituir a Política de Segurança da Informação no âmbito da Justiça Eleitoral do Ceará, doravante denominada PSI, na forma desta resolução, e em conformidade com:

I - a Política de Segurança da Informação (PSI) da Justiça Eleitoral, regulamentada pela Resolução TSE nº 23.644/2021;

II - a Política de Segurança Cibernética do Poder Judiciário (PSEC-PJ), regulamentada pela Resolução CNJ nº 396/2021;

III - a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

IV - os cinco controles críticos de SegCiber da versão 8 do *framework* do CIS referendados pelo Tribunal de Contas da União no Acórdão TCU-Plenário nº 1.768/2022; e

V - o Conjunto ABNT NBR ISO/IEC 27000.

Parágrafo único. As referências legais adicionais que embasam este normativo encontram-se relacionadas no anexo único.

CAPÍTULO II

DO OBJETIVO E DO ESCOPO

Art. 2º A Política de Segurança da Informação (PSI) é uma declaração formal acerca do compromisso com a proteção das informações de sua propriedade e/ou custodiada.

Parágrafo único. O propósito da PSI é direcionar o Tribunal Regional Eleitoral do Ceará no que diz respeito à gestão de riscos e ao tratamento dos incidentes relativos à Segurança da Informação e Comunicações (SIC), por meio da adoção de procedimentos e mecanismos, que visam à 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-CE, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de um Sistema de Gestão de Segurança da Informação (SGSI).

Art. 3º Esta PSI tem por objetivo instituir diretrizes estratégicas, responsabilidades e competências, de acordo com princípios fundamentais da segurança da informação conforme padrões internacionais, visando assegurar a confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade e conformidade dos dados, informações, documentos produzidos, armazenados ou transmitidos por quaisquer meios dos sistemas de informação do TRE-CE, contra ameaças e vulnerabilidades, de modo a preservar os seus ativos de informação, inclusive a imagem institucional.

Art. 4º Esta PSI se aplica às magistradas e aos magistrados, servidoras e servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiárias e estagiários, prestadoras e prestadores de serviço, colaboradoras e colaboradores, usuários externos, outros órgãos públicos ou entidades privadas contratadas ou com parcerias celebradas, acordos de cooperação de qualquer tipo, convênios e termos congêneres que fazem uso dos ativos de informação e de processamento no âmbito da Justiça Eleitoral do Ceará.

Parágrafo único. Os destinatários desta PSI, relacionados no *caput*, são corresponsáveis pela segurança da informação e comunicação, de acordo com os preceitos estabelecidos nesta resolução.

CAPÍTULO III DOS PRINCÍPIOS

Art. 5º As ações relacionadas à Segurança da Informação e Comunicação no TRE-CE são norteadas pelos seguintes princípios, assim definidos:

I - confidencialidade - garantia que a informação não seja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizada;

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 (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; e

VI - conformidade - garantia de que a informação produzida, enviada, modificada ou destruída obedece às normas, leis, estatutos, regulamentações ou obrigações contratuais, requisitos legais e quaisquer requisitos de segurança da informação.

CAPÍTULO IV DAS DEFINIÇÕES

Art. 6º Para efeito desta resolução, aplicam-se as seguintes definições:

I - ameaça: conjunto de fatores externos ou causa potencial de acidente indesejado, que pode resultar em dano para um sistema de informação ou para o TRE-CE;

II - ativo: qualquer componente humano, físico ou tecnológico que tenha ou gere valor para a instituição;

III - ativo de informação: meios de transmissão, armazenamento e processamento, os sistemas de informação, bem como os locais onde se encontram estes meios e as pessoas que a eles tem acesso;

IV - ETIR (Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais) - grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes computacionais;

V - CSI (Comissão de Segurança da Informação): tem o objetivo de coordenar e monitorar as ações atinentes à Segurança da Informação e Comunicação;

VI - GSI (Gestor de Segurança da Informação): servidora ou servidor do quadro efetivo da Justiça Eleitoral do Ceará, responsável pelas ações na área de segurança da

informação e comunicação, que detenha amplo conhecimento dos processos de negócio do Tribunal e especialista em gestão de segurança da informação, nos termos da Resolução do TSE nº 23.644/2021, subordinado diretamente à alta administração do órgão e desvinculado da área de TIC (Tecnologia da Informação e Comunicação), nos termos da Resolução do CNJ nº 396/2021;

VII - evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação;

VIII - incidentes em segurança da informação: é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

IX - incidentes de segurança da informação em redes computacionais: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de informação ou redes de computadores;

X - SIC (Segurança da Informação e Comunicação): ações que objetivam viabilizar e assegurar a confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade e conformidade das informações, abrangendo não somente os aspectos tecnológicos, mas também recursos humanos e processos;

XI - usuário: aquele que utiliza, de forma autorizada, recursos inerentes às atividades precípuas da Justiça Eleitoral do Ceará;

XII - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças; e

XIII - cibersegurança: é a prática de proteger ativos de informação computacional contra ameaças cibernéticas ou ataques maliciosos através de sistemas computacionais.

CAPÍTULO V DAS DIRETRIZES GERAIS

Art. 7º Deverão ser criadas, por meio da presidência ou por delegação, conforme o caso, normas, procedimentos, planos e/ou processos para os seguintes temas:

I - gestão de ativos;

II - controle de acesso físico e lógico;

III - gestão de riscos de segurança da informação;

IV - gestão de continuidade do negócio;

V - tratamento de incidentes de redes;

VI - gestão de incidentes de segurança da informação;

VII - auditoria e conformidade;

VIII - serviços de internet e correio eletrônico corporativo;

IX - desenvolvimento de sistemas seguros;

- X - processo de tratamento da informação;
- XI - geração e restauração de cópias de segurança (*backup*);
- XII - uso de recursos criptográficos;
- XIII - gestão de vulnerabilidades e padrões de configuração segura; e
- XIV - uso aceitável de recursos de TI.

Parágrafo único. Conforme necessidade e conveniência, poderão ser criados normativos sobre outras matérias.

CAPÍTULO VI DAS COMPETÊNCIAS

Art. 8º Compete a todas as unidades da Justiça Eleitoral do Ceará:

- I - cumprir as diretrizes dispostas por esta PSI, bem como as normas a ela complementares;
- II - promover cultura de segurança da informação e comunicações;
- III - executar as normas e procedimentos estabelecidos pela CSI;
- IV - gerenciar os ativos sob sua responsabilidade; e
- V - manter o sigilo/confidencialidade dos ativos de informações, quando determinado pela PSI.

Art. 9º Compete à Presidência nomear ou delegar à Diretoria-Geral:

- I - a criação da Comissão de Segurança da Informação;
- II - a criação do Comitê de Crises Cibernéticas;
- III - a criação da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
- IV - a criação do Comitê Gestor de Proteção de Dados;
- V - a expedição de portarias com normas, procedimentos, planos e/ou processos, regulamentando os temas do art. 7º; e
- VI - garantir e dar suporte ao Gestor de Segurança da Informação nas suas atividades.

Art. 10 Compete à Corregedoria Regional Eleitoral empreender medidas e expedir normas complementares para adequar as práticas cartorárias a esta PSI.

Art. 11 Compete à Diretoria-Geral:

- I - prover recursos financeiros necessários a implantação desta PSI, inclusive a exequibilidade do Plano de Continuidade de Negócio do Tribunal, abrangendo sua manutenção, treinamento e testes periódicos, quando no exercício da ordenação de despesas por delegação; e
- II - dar o devido encaminhamento administrativo às propostas da CSI de ações corretivas e disciplinares nos casos de violações de segurança.

Art. 12 Compete à Secretaria de Tecnologia da Informação:

I - propor dotação orçamentária específica para ações de segurança da informação e comunicações;

II - garantir o alinhamento estratégico entre esta PSI, suas normatizações, ações de segurança da informação e comunicação;

III - fornecer suporte material e estrutural necessário à operacionalização da PSI e suas normatizações;

IV - subsidiar a CSI com as informações técnicas necessárias aplicadas à segurança da informação e comunicação; e

V - garantir o mínimo de pessoal técnico qualificado na execução da PSI na cibersegurança.

Art. 13 Compete à Secretaria de Administração:

I - implantar controles de acesso e proteção contra ameaças externas ou decorrentes do meio ambiente;

II - assegurar que os colaboradores das prestadoras de serviços contratadas conheçam suas atribuições e responsabilidades em relação à segurança da informação e comunicação; e

III - oferecer estrutura física adequada, obedecendo aos padrões de segurança.

Art. 14 Compete à Secretaria de Gestão de Pessoas:

I - apoiar a Comissão de Segurança da Informação na missão de assegurar que as magistradas e os magistrados, membras e membros do Ministério Público, servidoras e servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo e estagiárias e estagiários conheçam suas atribuições e responsabilidades em relação à segurança da informação e comunicação;

II - promover a capacitação das(os) servidoras e servidores que integram a estrutura da gestão da segurança da informação, no que for pertinente.

III - informar à Secretaria de Tecnologia da Informação toda e qualquer movimentação de temporárias(os) e/ou estagiárias(os), e admissão/demissão/afastamentos de servidoras(es)/terceirizadas(os), para que possam ser cadastradas(os) ou excluídas(os) nos sistemas do TRE/CE;

IV - aplicar, na gestão de pessoas, normas definidas pela PSI, no que couber;

V - observar a aplicação da Lei nº 13.709, de 14 de Agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), com apoio do Comitê Gestor de Proteção de Dados Pessoais (CGPD);

VI - prover, junto ao Gestor de Segurança da Informação, treinamento às(aos) colaboradoras e colaboradores do TRE-CE.

Art. 15 Compete à Assessoria de Comunicação em conjunto com a Comissão de Segurança da Informação:

I - promover campanhas de conscientização sobre a importância da Segurança da Informação e Comunicações; e

II - divulgar esta PSI.

Art. 16 Compete à Comissão de Segurança da Informação, sem prejuízo de suas demais competências:

I - aprovar as normas e procedimentos, visando à regulamentação das diretrizes fixadas nesta PSI da Justiça Eleitoral do Ceará, em conformidade com a legislação vigente;

II - definir o plano de monitoramento e auditoria periódica da segurança da informação, nos termos desta PSI;

III - promover a análise dos relatórios e recomendar ações apropriadas para os incidentes de segurança identificados;

IV - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações; e

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

Art. 17 Compete ao Gestor de Segurança da Informação, sem prejuízo do disposto na Política de Segurança da Informação da Justiça Eleitoral, instituída pelo TSE:

I - instituir e gerir o Sistema de Gestão de Segurança da Informação - SGSI;

II - acompanhar a aplicação desta PSI e suas normatizações;

III - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

IV - coordenar as atividades da ETIR (Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais);

V - assessorar a alta administração do órgão do Poder Judiciário Eleitoral do Ceará em todas as questões relacionadas à segurança da informação;

VI - consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

VII - propor normas internas relativas à segurança da informação;

VIII - auxiliar na aplicação da LGPD;

IX - acompanhar as mudanças de legislação aplicada à segurança da informação;

X - planejar treinamentos e conscientização às(aos) servidoras e servidores, magistradas e magistrados e colaboradoras e colaboradores da Justiça Eleitoral do Ceará;

XI - elaborar ações junto à Secretaria de Tecnologia da Informação (STI) no âmbito da cibersegurança;

XII - compor o Comitê de Crises Cibernéticas da Justiça Eleitoral do Ceará;

XIII - presidir a Comissão de Segurança da Informação da Justiça Eleitoral do Ceará; e

XIV - manter contatos apropriados com grupos de interesses especiais ou outros fóruns especializados de segurança da informação e associações profissionais, a fim de compartilhar e trocar informações sobre novas tecnologias, produtos, ameaças ou vulnerabilidades.

Parágrafo único. A(o) titular da Assessoria de Segurança da Informação - ASEGI, ou sua(eu) substituta(o), acumulará a função de Gestor de Segurança da Informação - GSI da Justiça Eleitoral do Ceará.

CAPÍTULO VII DAS SANÇÕES E PENALIDADES

Art. 18 O descumprimento ou violação das regras previstas na PSI pela(o) usuária(o) resultará na aplicação das sanções previstas em regulamentações internas e legislação vigente.

CAPÍTULO VIII DA ATUALIZAÇÃO

Art. 19 Esta norma e os instrumentos normativos gerados a partir dela deverão ser revisados sempre que se fizer necessário.

CAPÍTULO IX DAS DISPOSIÇÕES FINAIS

Art. 20 A PSI instituída por esta resolução deverá ser publicada e amplamente promovida, garantindo seu amplo conhecimento para adequado usufruto dos benefícios e assunção das responsabilidades sobre os ativos de informação do Tribunal Regional Eleitoral do Ceará.

Art. 21 O processo de aquisição de bens e serviços relacionados a ativos de informação no TRE-CE deverá observar a conformidade desta PSI.

Art. 22 Casos omissos desta PSI serão resolvidos pela CSI.

Art. 23 Esta resolução entra em vigor na data da sua publicação, revogando-se a Resolução TRE-CE nº 671/2017.

Sala das Sessões do Tribunal Regional Eleitoral do Ceará, em Fortaleza, aos 24 dias do mês de outubro de 2022.

Desembargador Inacio de Alencar Cortez Neto – PRESIDENTE, Desembargador Raimundo Nonato Silva Santos - VICE-PRESIDENTE, Jurista David Sombra Peixoto – JUIZ, Jurista Kamile Moreira Castro – JUÍZA, Juiz Federal George Marmelstein Lima – JUIZ, Juiz de Direito Raimundo Deusdeth Rodrigues Júnior – JUIZ, Juiz de Direito Roberto Soares Bulcão Coutinho – JUIZ, Procurador da República Samuel Miranda Arruda - PROCURADOR REGIONAL ELEITORAL.

Publicada na edição do DJE n.º 248 de 25.10.2022, pp. 10 a 17.

ANEXO ÚNICO

REFERÊNCIAS LEGAIS E NORMATIVAS

As ações do SGSI do TRE-CE deverão observar os seguintes requisitos legais e normativos:

I - Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

II - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;

III - Lei nº 9.983, de 14 de julho de 2000, que dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

IV - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;

V - Lei nº 12.737, de 20 de novembro de 2012, que dispõe sobre a tipificação criminal de delitos informáticos;

VI - Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

VII - Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

VIII - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, *caput*, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional;

IX - Decreto nº 5.482, de 30 de junho de 2005, que dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da administração pública federal, por meio da Rede Mundial de Computadores (Internet);

X - Resolução nº 370, de 28 de janeiro de 2021, do Conselho Nacional de Justiça (CNJ), que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

XI - Resolução nº 396, de 7 de junho de 2021, do Conselho Nacional de Justiça, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

XII - Resolução nº 23.644, de 1º de julho de 2021, do Tribunal Superior Eleitoral, que institui a Política de Segurança da Informação no âmbito da Justiça Eleitoral;

XIII - Resolução nº 601, de 21 de outubro de 2015, que institui o Código de Ética dos servidores do Tribunal Regional Eleitoral do Ceará;

XIV - Norma ABNT NBR/ISO/IEC 27002:2005, que institui o código de melhores práticas para Gestão de Segurança da Informação e Comunicações;

XV - Norma ABNT NBR/ISO/IEC 27001:2006, que estabelece os elementos de um Sistema de Gestão de Segurança da Informação e Comunicações; e

XVI - Norma ABNT NBR ISO/IEC 27005:2008, que fornece as diretrizes para a Gestão de Riscos de Segurança da Informação e Comunicações.