TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO

RESOLUÇÃO Nº 1001/2017

Dispõe sobre a Política de Segurança da Informação do Tribunal Regional Eleitoral do Rio de Janeiro (PSI/TRE-RJ).

O TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO, no uso de suas atribuições legais e regimentais,

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 as informações neste Tribunal são armazenadas em diferentes suportes, veiculadas de diferentes formas e, portanto, vulneráveis a incidentes como desastres naturais, acessos não autorizados, mau uso, extravio, furto e falhas de equipamentos, dentre outros;

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 as diretrizes sobre segurança da informação expedidas pelo Conselho Nacional de Justiça para todos os órgãos do Poder Judiciário;

CONSIDERANDO os Direitos e garantias individuais e coletivas assegurados nos incisos IX, X, XII, XIV e XXXIII e LXXII do art.5º da Constituição Federal de 1988, bem como aos princípios previstos no art. 37 do mesmo diploma legal;

CONSIDERANDO a Lei nº 9.983, de 14 de julho de 2000, que altera o Código Penal para acrescer dispositivo relacionado à responsabilidade criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública, bem como a Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações; e

CONSIDERANDO, ainda, a necessidade de incorporar à Política de Segurança da Informação deste Tribunal as normas, definições e conceitos advindos com a publicação da Resolução TSE n.º 23.501/2016, que instituiu a Política de Segurança da Informação no âmbito da Justiça Eleitoral,

RESOLVE:

Art. 1º A Política de Segurança da Informação do Tribunal Regional Eleitoral do Rio de Janeiro (PSI/TRE-RJ), instituída pela Resolução TRE/RJ n.º 943/2016, passa a vigorar nos termos da presente Resolução.

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.

CAPÍTULO I

DAS DEFINIÇÕES E CONCEITOS TÉCNICOS

Art. 2º Para os efeitos desta Resolução e de suas regulamentações, entende-se por:

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 - documento: unidade de registro de informações, qualquer que seja o formato ou o suporte;

XVII - ETIR - Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais: grupo de pessoas com a responsabilidade de receber, analisar,

classificar, tratar e responder as notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

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 - gestor de ativo da informação: responsável por garantir o uso adequado do ativo de informação, a definição de critérios de acesso, classificação, tempo de vida e normas específicas de seu uso;

XXI - gestor de processo: responsável por acompanhar e controlar o desempenho de um processo, a fim de garantir seus resultados;

XXII - 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;

XXIII - 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;

XXIV - 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;

XXV - Plano de Continuidade de Negócios (PCN): 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;

XXVI - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

XXVII - recurso: além da própria informação, é todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;

XXVIII - recurso criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

XXIX - 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;

XXX - risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;

XXXI - 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;

XXXII - tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XXXIII - 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;

XXXIV - usuário interno: qualquer pessoa física que faça uso de informações e exerça atividade na Justiça Eleitoral do Rio de Janeiro, ainda que temporariamente, com ou sem remuneração.

XXXV - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO II

DOS PRINCÍPIOS

Art. 3º São princípios que regem a PSI/TRE-RJ:

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: propriedade que garante que a informação mantém todas as características originais estabelecidas pelo proprietário;

III - autenticidade: propriedade que garante que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade; (na do TSE está no capítulo dos conceitos e definições);

IV - irretratabilidade (ou não repúdio): garantia de que a pessoa se responsabilize por ter assinado ou criado a informação;

V - disponibilidade: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada.

CAPÍTULO III

DO OBJETIVO

Art. 4º A PSI/TRE-RJ tem por finalidade dotar a Administração de instrumentos normativos e organizacionais adequados a assegurar a confidencialidade, a integridade, a autenticidade, a irretratabilidade e a disponibilidade no uso dos dados e das informações, no interesse da Instituição, promovendo a continuidade de seu negócio e contribuindo para o alcance dos seus objetivos estratégicos.

Art. 5º São objetivos da PSI /TRE-RJ:

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

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

III - 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 de recursos humanos em segurança da informação.

CAPÍTULO IV

DA ESTRUTURA NORMATIVA

Art. 6º A estrutura normativa da segurança da informação, no âmbito do Tribunal Regional Eleitoral do Rio de Janeiro, seguirá a seguinte conformação:

I - Política de Segurança da Informação (Política), que contempla a estrutura, diretrizes e responsabilidades referentes à Segurança da Informação e é corporificada pela presente Resolução e por atos da Presidência do TRE-RJ;

II - Normas de Segurança da Informação (Normas), disciplinadas mediante atos normativos da Diretoria-Geral, que contemplam obrigações a serem seguidas de acordo com as diretrizes estabelecidas na Política de Segurança; e

III - Procedimentos de Segurança da Informação (Procedimentos), normatizados mediante Instrução Normativa da Diretoria-Geral, que contemplam regras operacionais de acordo com o disposto nas diretrizes e normas de segurança estabelecidas, permitindo sua utilização nas atividades do órgão.

CAPÍTULO V

DA COMISSÃO PERMANENTE DE SEGURANÇA DA INFORMAÇÃO

Art. 7º A Comissão Permanente de Segurança da Informação da Justiça Eleitoral do Rio de Janeiro (ComSI/TRE-RJ), subordinada à Presidência do Tribunal, será composta por servidores ocupantes de cargo efetivo da Justiça Eleitoral, sendo, pelo menos, um servidor da Presidência, um da Vice-Presidência e Corregedoria Regional Eleitoral, um da Diretoria-Geral, um da Assessoria de Comunicação Social, um da Assessoria de Segurança e um de cada Secretaria, indicados pelos respectivos titulares das unidades e, posteriormente, designados pela Presidência.

Parágrafo único O ato de designação da Comissão de Segurança da Informação indicará o seu presidente, o substituto eventual deste e o secretário.

Art. 8º Compete à Comissão de Segurança da Informação:

I - propor melhorias a esta PSI;

II - propor normas, procedimentos, planos e/ou processos, nos termos do art. 6º, 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 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 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 Redes Computacionais (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, em conjunto com o Gestor de Segurança da Informação.

§1º A ComSI/TRE-RJ poderá requisitar temporariamente servidores das unidades do Tribunal para colaborar com as atividades da Comissão.

§2º Sempre que necessário, a ComSI/TRE-RJ poderá solicitar aos titulares das unidades informações pertinentes à segurança da informação.

CAPÍTULO VI

DA EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES DE REDES COMPUTACIONAIS

Art. 9º Deverá ser instituída 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.**

Parágrafo único Caberá ainda à ETIR elaborar o Processo de Tratamento e Resposta a Incidentes em Redes de Computadores no âmbito do Tribunal Eleitoral.

CAPÍTULO VII

DA COMPETÊNCIA DO GESTOR DE SEGURANÇA DA INFORMAÇÃO

Art. 10 Deverá ser nomeado um Gestor de Segurança da Informação, com as seguintes responsabilidades:

I - receber, analisar e manifestar-se preliminarmente nos procedimentos relacionados à segurança da informação;

II - propor normas relativas à segurança da informação à Comissão de Segurança da Informação, elaboradas por iniciativa própria ou após avaliação de normas propostas pelas demais unidades do Tribunal;

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

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

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

VI - Responder pela segurança da informação, em conjunto com a Comissão de Segurança da Informação.

§ 1º 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.

§ 2º Sempre que necessário, o Gestor de Segurança da Informação poderá solicitar aos titulares das unidades informações pertinentes à segurança da informação.

§ 3º O Gestor de Segurança da Informação deverá ser servidor do quadro, que não componha a ComSI, e que detenha amplo conhecimento dos processos de negócio do Tribunal e do tema em foco.

§ 4º O ato de nomeação do Gestor de Segurança da Informação indicará também o seu substituto eventual.

CAPÍTULO VIII

DAS COMPETÊNCIAS DAS UNIDADES

Art. 11 Compete à Presidência do TRE-RJ:

I - aprovar os Planos de Continuidade de Negócio (PCN);

II - apoiar a aplicação das ações estabelecidas nesta PSI;

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

a) dos componentes da Comissão de Comissão de Segurança da Informação, nos termos do art. 7º desta Resolução;

b) do Gestor de Segurança da Informação e seu substituto, nos termos do art. 10;

c) de integrantes da ETIR, nos termos do art. 9º.

Art. 12 Compete à Assessoria de Comunicação Social, com a Comissão de Segurança da Informação:

I - promover campanhas de conscientização sobre a importância da segurança da informação;

II - divulgar esta PSI;

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

Art. 13 Compete à Assessoria de Segurança:

I - implantar controles de ambientes físicos visando prevenir danos, furtos, roubos, interferências e acessos não autorizados às instalações e ao patrimônio da Justiça Eleitoral do Rio de Janeiro;

II - implantar controles e proteção contra ameaças externas ou decorrentes do meio ambiente, como incêndios, enchentes, explosões, perturbações da ordem pública e desastres naturais ou causados pelo homem.

Art. 14 Compete à Escola Judiciária Eleitoral apoiar a Comissão de Segurança da Informação na missão de assegurar que os magistrados conheçam suas atribuições e responsabilidades em relação à segurança da informação.

Art. 15 Compete à Vice-Presidência e Corregedoria Regional Eleitoral:

I - 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;

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

Art. 16 Compete ao Diretor-Geral da Secretaria do Tribunal:

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

II - decidir sobre suspensão cautelar do serviço ou do acesso de usuário a ativo da informação da Justiça Eleitoral do Rio de Janeiro, comunicada pelo Gestor de Segurança da Informação, com prosseguimento das demais medidas cabíveis;

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

IV - apoiar a aplicação das ações estabelecidas nesta PSI;

V - viabilizar financeiramente as ações de implantação desta PSI, inclusive a exequibilidade do Plano de Continuidade de Negócios do Tribunal, abrangendo sua manutenção, treinamento e testes periódicos;

VI - designar os gestores de ativo da informação, sistema ou serviço.

§1º Os gestores de ativo da informação de que trata o inciso VI serão vinculados à função ou ao cargo da respectiva unidade e, no caso de processos mapeados, ao gestor do processo, quanto aos ativos de informação inerentes ao escopo do processo e que transcendam às atribuições das unidades envolvidas.

§2º O gestor de ativo da informação poderá nomear custodiante como responsável pelo processamento ou armazenamento da informação nas tarefas de rotina.

Art. 17 Compete à Secretaria de Tecnologia da Informação, na sua área de atuação:

I - prover o apoio necessário à implementação e compreensão da PSI/TRE-RJ;

II - executar as orientações técnicas e procedimentos estabelecidos pela ComSI/TRE-RJ;

III - prover os ativos de processamento necessários ao cumprimento da PSI/TRE-RJ;

IV - subsidiar a Comissão de Segurança da Informação com o conhecimento de cunho tecnológico, aplicado à execução da PSI/TRE-RJ;

V - 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;

VI - disponibilizar e gerenciar a infraestrutura necessária aos processos de trabalho da ETIR.

Art. 18 Compete à Secretaria de Administração, na sua área de atuação:

I - 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;

II - executar as orientações técnicas e procedimentos estabelecidos pela Comissão de Segurança da Informação;

III - assegurar que os empregados das empresas prestadoras de serviço contratadas conheçam suas atribuições e responsabilidades em relação à segurança da informação.

Art. 19 Compete à Secretaria de Gestão de Pessoas, na sua área de atuação:

I - apoiar a Comissão de Segurança da Informação na missão de assegurar que os servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, colaboradores e estagiários conheçam suas atribuições e responsabilidades em relação à segurança da informação;

II - adotar as medidas necessárias, quando da mudança de lotação, afastamentos ou desligamento de pessoal, e comunicar o fato às demais unidades do Tribunal com vistas à pertinente remoção dos acessos às informações da Justiça Eleitoral do Rio de Janeiro;

III - capacitar regularmente os servidores que atuam diretamente com controles de segurança da informação no que for pertinente;

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

Art. 20 Compete à Secretaria de Controle Interno e Auditoria:

I - incluir no escopo do Plano Anual de Auditoria, nos termos estabelecidos no art. 42, a análise do cumprimento desta PSI, seus regulamentos e demais normativos de segurança vigentes;

II - realizar auditorias conforme Plano Anual de Auditoria;

III - executar as orientações técnicas e procedimentos estabelecidos pela Comissão de Segurança da Informação.

Art. 21 Compete à unidade responsável pela Gestão da Informação:

I - regulamentar e coordenar o processo de classificação da informação no âmbito do Tribunal;

II - executar as orientações técnicas e os procedimentos estabelecidos.

Art. 22 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 de Segurança da Informação.

Art. 23 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/TRE-RJ;

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 da PSI/TRE-RJ 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 da PSI/TRE-RJ;

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 da PSI/TRE-RJ;

VII - propor ao Gestor da Segurança da Informação procedimentos visando à regulamentação e operacionalização das diretrizes e normas de segurança apresentadas pela PSI/TRE-RJ.

Art. 24 Compete a todos os usuários:

I - responder por toda atividade executada com o uso de sua identificação;

II - ter pleno conhecimento desta PSI;

III - reportar tempestivamente ao Gestor de Segurança da Informação 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 - observar o adequado manuseio e armazenamento de documentos e processos;

VI - executar as orientações técnicas e os procedimentos estabelecidos pela Comissão de Segurança da Informação;

VII - gerenciar os ativos sob sua responsabilidade.

Art. 25 A Presidência, a Vice-Presidência e Corregedoria Regional Eleitoral, as Assessorias, a Diretoria-Geral, as Secretarias e as Comissões Permanentes, sob a coordenação do Gestor de Segurança da Informação, serão co-responsáveis pela elaboração de Plano de Continuidade de Negócio à aprovação da Presidência do Tribunal.

Parágrafo único A ComSI/TRE-RJ analisará o Plano de Continuidade de Negócio e emitirá parecer recomendando a sua aprovação, quando em conformidade com as normas técnicas e legislação de segurança da informação.

Art. 26 Compete à Presidência, Vice-Presidência e Corregedoria Regional Eleitoral e Diretoria-Geral a supervisão do Processo de Gestão de Riscos.

Parágrafo único. Compete ao Gestor de Segurança da Informação coordenar a implementação do Processo de Gestão de Riscos.

CAPÍTULO IX

DAS DIRETRIZES

Art. 27 Deverão ser criadas, conforme o caso, normas, procedimentos, planos e/ou processos, para as seções elencadas neste capítulo.

Seção I

Do Processo de Tratamento da Informação

Art. 28 Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo Tribunal Regional Eleitoral do Rio de Janeiro deve ser protegida, de acordo com a Política de que trata esta Resolução, a legislação em vigor e as normas e procedimentos relacionados.

Art. 29 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 ciclo de vida, contemplando o conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Parágrafo único O conjunto das ações referentes ao tratamento da informação será agrupado nas seguintes fases:

I - produção e recepção: refere-se à fase inicial do ciclo de vida e compreende produção, recepção ou custódia e classificação da informação;

II - organizações: refere-se ao armazenamento, arquivamento e controle da informação;

III - uso e disseminação: refere-se à utilização, acesso, reprodução, transporte, transmissão e distribuição da informação;

IV - destinações: refere-se à fase final do ciclo de vida da informação e compreende avaliação, destinação ou eliminação da informação.

Seção II

Da Gestão de ativos

Art. 30 Toda e qualquer informação produzida ou custodiada pela Justiça Eleitoral deve ser classificada em função do seu grau de confidencialidade, criticidade,

disponibilidade, integridade e prazo de retenção, devendo ser protegida, de acordo com a regulamentação de classificação da informação.

Parágrafo único Os procedimentos para as operações de armazenamento, divulgação, reprodução, transporte, recuperação e descarte da informação devem ser definidos de acordo com a sua classificação.

Art. 31 As informações produzidas por usuários, no exercício de suas funções, são patrimônio intelectual da Justiça Eleitoral, e não cabe a seus criadores qualquer forma de direito autoral.

Art 32 É vedado o uso de ativos e recursos da Justiça Eleitoral para obter proveito pessoal ou de terceiro, ou para constranger, assediar, ofender, caluniar, ameaçar ou causar prejuízos a qualquer pessoa física ou jurídica, bem como para veicular opiniões político-partidárias.

Art. 33 É vedado que apenas um usuário possua controle exclusivo de um processo de negócio ou recurso.

Art. 34 Todos os ativos de informação e de processamento do TRE-RJ devem ser inventariados, classificados, atualizados periodicamente e mantidos em condição de uso.

Parágrafo único Cada ativo de informação e de processamento deverá ter uma unidade responsável, com atribuições claramente definidas.

Art. 35 O processo de classificação da informação deverá ser regulamentado e coordenado pela unidade ou comissão responsável pela gestão da informação.

Art. 36 Todos os recursos tecnológicos, sistemas, informações e serviços disponibilizados aos usuários internos e externos são de propriedade do Tribunal Regional Eleitoral do Rio de Janeiro, não podendo ser interpretados como sendo de uso pessoal.

Parágrafo único O uso dos recursos tecnológicos, sistemas, informações e serviços deve ser monitorado e os registros, assim obtidos, poderão ser utilizados para detectar atividades não autorizadas.

Seção III

Do Controle de acessos

Art. 37 Todo usuário deve possuir identificação pessoal, intransferível e, quando aplicável, com validade estabelecida, de forma a assegurar a responsabilidade de cada usuário por suas ações.

Parágrafo único Devem ser adotados mecanismos que garantam a integridade e autenticidade da identificação do usuário.

Art. 38 O acesso às informações produzidas ou custodiadas pela Justiça Eleitoral que não sejam de domínio público deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades dos destinatários desta PSI, na forma descrita no art. 46.

§ 1º As permissões de acesso devem ser bloqueadas, em caso de afastamento provisório, e revogadas, em caso de desligamento do usuário.

§ 2º Qualquer outra forma de uso que extrapole as atribuições necessárias ao desempenho das atividades necessitará de prévia autorização formal.

§ 3º 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.

Seção IV

Da Gestão de Riscos

Art. 39 Deverá ser estabelecido Processo de Gestão de Riscos do Tribunal, visando à identificação, avaliação e posterior tratamento e monitoramento dos riscos considerados críticos para a segurança da informação.

Parágrafo único Processo de Gestão de Riscos deverá ser revisado periodicamente.

Seção V

Da Gestão da Continuidade de Negócios

Art. 40 Deverá ser elaborado Plano de Continuidade de Negócios que estabeleça procedimentos e defina estrutura mínima de recursos para que se desenvolva uma resiliência organizacional capaz de garantir o fluxo das informações críticas em momento de crise e salvaguardar o interesse das partes interessadas, a reputação e a marca da organização.

Parágrafo único O Plano de Continuidade de Negócios deverá ser testado e revisado periodicamente.

Seção VI

Do Tratamento de Incidentes de Rede

Art. 41 Deverá ser elaborado pela ETIR um Processo de Tratamento e Resposta a Incidentes em Redes de Computadores, visando impedir, interromper ou minimizar o impacto de uma ação maliciosa ou acidental.

Seção VII

Da Gestão de Incidentes de Segurança da Informação

Art. 42 A gestão de incidentes em segurança da informação tem por objetivo assegurar que fragilidades e incidentes em segurança da informação sejam identificados, permitindo a tomada de ação corretiva em tempo hábil.

Parágrafo único Os usuários são responsáveis por:

I - reportar tempestivamente ao Gestor de Segurança da Informação os incidentes em segurança da informação de que tenham ciência ou suspeita;

II - colaborar, em suas áreas de competência, na identificação e no tratamento de incidentes em segurança da informação.

Seção VIII

Da Auditoria

Art. 43 Deverá ser incluída no escopo do Plano Anual de Auditoria análise do correto cumprimento desta PSI, seus regulamentos e demais normativos de segurança vigentes.

Parágrafo único A inclusão no escopo do Plano Anual de Auditoria deve ser realizada, no mínimo, a cada dois anos e deve abranger uma ou mais normas, procedimentos, planos e/ou processos estabelecidos.

Seção IX

Dos Serviços de Internet e Do Correio Eletrônico Corporativo

Art. 44 Os serviços de acesso à Internet e de correio eletrônico corporativo disponibilizados aos usuários são considerados de propriedade da Justiça Eleitoral e passíveis de monitoramento.

Seção X

Do Desenvolvimento de Sistemas Seguros

Art. 45 O Processo de Desenvolvimento de Software dos Tribunais Eleitorais deverá contemplar atividades específicas que garantam maior segurança para os sistemas utilizados, de forma a preservar o ambiente tecnológico, assim como prevenir possíveis incidentes de segurança com os dados desses sistemas ou com a infraestrutura utilizada.

Seção XI

Do Uso de Recursos Criptográficos

Art. 46 Toda a 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 X

DAS RESPONSABILIDADES

Art. 47 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 dos ativos de informação e de processamento no âmbito da Justiça Eleitoral fluminense.

Parágrafo único Todos aqueles relacionados no caput deste artigo são co-responsáveis pela segurança da informação, devendo, para tanto, conhecer e seguir a PSI/TRE-RJ.

Art. 48 Compete aos usuários:

I - proteger as informações sigilosas e pessoais obtidas em decorrência do exercício de suas atividades;

II - reportar tempestivamente ao Gestor de Segurança da Informação quaisquer falhas ou indícios de falhas de segurança de que tenha conhecimento ou suspeita;

III - disponibilizar os dados e informações necessários ao desempenho das atividades da Justiça Eleitoral do Rio de Janeiro;

IV - guardar sigilo de senhas e códigos fornecidos para utilização dos equipamentos e sistemas da Justiça Eleitoral do Rio de Janeiro, adotando medidas para manutenção de sua confidencialidade;

V - utilizar as informações e os dados a que tem acesso no exercício de suas atividades para uso exclusivo de suas atribuições funcionais;

VI - responder por toda atividade executada com o uso de sua identificação;

VII - ter pleno conhecimento desta PSI;

VIII- executar as orientações técnicas e os procedimentos estabelecidos pela Comissão de Segurança da Informação;

IX - gerenciar os ativos sob sua responsabilidade.

Art. 49 O descumprimento desta PSI será objeto de apuração pela unidade competente do Tribunal 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.

CAPÍTULO XI

DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 50 Esta PSI e demais normas, procedimentos, planos e/ou processos deverão ser publicados na Intranet do Tribunal pela Comissão de Segurança da Informação.

Art. 51 As iniciativas relacionadas à segurança da informação comporão o Plano Diretor da Estratégia do Tribunal Regional Eleitoral do Rio de Janeiro e serão priorizadas pelo Comitê de Gestão Estratégica.

Art. 52 Enquanto não for efetuada a designação de que trata o inciso VI do artigo 16 da presente norma, o gestor da informação, do sistema ou do serviço disponibilizado será o titular da principal unidade usuária do ativo.

Parágrafo único Nos casos em que não for possível associar o ativo a uma única unidade, a gestão poderá ser compartilhada por duas ou mais unidades dentre as principais usuárias do ativo.

Art. 53 A PSI/TRE-RJ, as normas e os procedimentos de segurança da informação, bem como o Plano de Continuidade do Negócio, devem ser analisados criticamente, em intervalos mínimos de dois anos e máximos de quatro anos, ou quando mudanças significativas ocorrerem, para assegurar sua contínua pertinência, adequação, eficácia e aprimoramento.

Parágrafo único Qualquer usuário poderá encaminhar ao Gestor de Segurança da Informação ou à ComSI/TRE-RJ, para apreciação, sugestão para melhoria da Política, Normas e Procedimentos de Segurança da Informação.

Art. 54 As normas internas do TRE-RJ 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 18 (dezoito) meses contados a partir da data da publicação desta Resolução.

Art. 55 Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres, celebrados pelo Tribunal, devem observar, no que couber, as diretrizes, normas e procedimentos estabelecidos na PSI/TRE-RJ.

Art. 56 Os casos omissos desta PSI serão resolvidos pela Comissão e Segurança da Informação, juntamente com o Gestor de Segurança da Informação.

Art. 57 Revogam-se as disposições em contrário, em especial a Resolução TRE-RJ n.º 943/2016.

Art. 58 A presente Resolução entra em vigor na data de sua publicação.

Sala das Sessões, em 18 de dezembro de 2017.

Desembargador CARLOS EDUARDO DA FONSECA PASSOS
Presidente

Publicada no DJE/RJ de 26/12/2017.