TRIBUNAL SUPERIOR ELEITORAL

RESOLUÇÃO Nº 23.501

PROCESSO ADMINISTRATIVO Nº 416-03.2016.6.00.0000 – CLASSE 26 – BRASÍLIA – DISTRITO FEDERAL

Relator: Ministro Gilmar Mendes
Interessado: Tribunal Superior Eleitoral

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

O TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições e

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

CONSIDERANDO que as informações na Justiça Eleitoral são armazenadas em diferentes formas, veiculadas em diferentes meios físicos e eletrônicos, portanto vulneráveis a incidentes como desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto;

CONSIDERANDO a importância da adoção de boas práticas relacionadas à proteção da informação preconizadas pelas normas NBR ISO/IEC 27001:2013, NBR ISO/IEC 27002:2013, NBR ISO/IEC 27005:2011 e as Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário de 2012, às quais a Política de Segurança da Informação (PSI) da Justiça Eleitoral deverá estar alinhada;

CONSIDERANDO a edição do Acórdão-TCU nº 1233/2012-plenário, que recomenda ao Conselho Nacional de Justiça a

promoção de ações para a melhoria da governança de tecnologia da informação em virtude do resultado de diagnóstico de maturidade e aderência de processos de segurança da informação;

CONSIDERANDO o Decreto nº 3.505/2000, que institui a obrigatoriedade do estabelecimento de Políticas de Segurança da Informação nos órgãos da Administração Pública Federal;

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

CONSIDERANDO a Resolução nº 211/2015 do Conselho Nacional de Justiça que dispõe sobre os requisitos de nivelamento de tecnologia da informação no âmbito do Poder Judiciário;

CONSIDERANDO a Resolução TSE nº 23.379/2012, que dispõe sobre o Programa de Gestão Documental no âmbito da Justiça Eleitoral;

CONSIDERANDO a necessidade de orientar a condução de Políticas de Segurança da Informação no âmbito da Justiça Eleitoral;

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.

CAPÍTULO I

DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para os 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 - 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;

VIII - ciclo de vida da informação: ciclo formado pelas fases de produção, recepção, organização, uso, disseminação e destinação;

IX - 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;

X - confidencialidade: propriedade da informação que garante que ela não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem a devida autorização;

XI - 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;

XII - decifração: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

XIII - disponibilidade: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada;

XIV - 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;

XV - 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;

XVI - 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;

XVII - 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;

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

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

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

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

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

XXIII - 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;

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

XXV - 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;

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

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

XXVIII - 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 se alinha às estratégias da Justiça Eleitoral e tem como princípio norteador a garantia da integridade, da autenticidade, da

confidencialidade, da disponibilidade e da irretratabilidade dos ativos de informação e de processamento.

CAPÍTULO III

DO ESCOPO

Art. 4º São objetivos da PSI da Justiça Eleitoral:

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.

Art. 5º Esta PSI se aplica a todos os magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço, colaboradores e usuários externos que fazem uso dos ativos de informação e de processamento no âmbito da Justiça Eleitoral.

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

CAPÍTULO IV

DAS DIRETRIZES GERAIS

Art. 6º Deverão ser criadas, conforme o caso, normas, procedimentos, planos e/ou processos, para as seções elencadas neste capítulo.

Parágrafo único. Conforme necessidade e conveniência de cada Tribunal Eleitoral, poderão ser criados normativos sobre outros temas.

Seção I

Da Gestão de Ativos

Art. 7º Todos os ativos de informação e de processamento da Justiça Eleitoral deverão ser inventariados, classificados, atualizados periodicamente e mantidos em condições de uso.

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

Art. 8º O processo de classificação da informação deverá ser regulamentado e coordenado pela unidade ou comissão responsável pela gestão da informação.

Art. 9º 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. 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. 10. É vedado o uso dos ativos da Justiça Eleitoral para obter proveito pessoal ou de terceiro, bem como para veicular opiniões político-partidárias.

Seção II

Do Controle de Acessos

Art. 11. 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 *caput* do art. 5º.

§ 1º Qualquer outra forma de uso que extrapole as atribuições necessárias ao desempenho das atividades necessitará de prévia autorização formal.

§ 2º 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.

Art. 12. Todo usuário deverá possuir identificação pessoal e intransferível, qualificando-o, inequivocamente, como responsável por qualquer atividade desenvolvida sob essa identificação.

Seção III

Da Gestão de Riscos

Art. 13. Deverá ser estabelecido Processo de Gestão de Riscos de ativos de informação e de processamento do Tribunal Eleitoral, visando à identificação, avaliação e posterior tratamento e monitoramento dos riscos considerados críticos para a segurança da informação.

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

Seção IV

Da Gestão da Continuidade de Negócios

Art. 14. 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 V

Do Tratamento de Incidentes de Rede

Art. 15. Deverá ser elaborado 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 VI

Da Gestão de Incidentes de Segurança da Informação

Art. 16. 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; e

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

Seção VII

Da Auditoria e Conformidade

Art. 17. Deverá ser incluída no escopo do Plano Anual de Auditoria e Conformidade 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 e Conformidade deve ser realizada, no mínimo, a cada dois anos e deve abranger uma ou mais normas, procedimentos, planos e/ou processos estabelecidos.

Seção VIII

Dos Serviços de Internet e Do Correio Eletrônico Corporativo

Art. 18. 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 IX

Do Desenvolvimento de Sistemas Seguros

Art. 19. 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 X

Do Uso de Recursos Criptográficos

Art. 20. 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.

Seção XI

Do Processo de Tratamento da Informação

Art. 21. 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.

CAPÍTULO V

DA ESTRUTURA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 22. Deverá ser constituída, no âmbito dos Tribunais Eleitorais, Comissão de Segurança da Informação, subordinada à Presidência do Tribunal, composta, no mínimo, por representantes da Presidência, da Corregedoria, da Diretoria-Geral, de cada Secretaria e da Assessoria de Comunicação Social ou da unidade que desempenhe essa atividade.

Art. 23. 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.

Art. 24. Caberá, especificamente, à Comissão de Segurança da Informação do Tribunal Superior Eleitoral:

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

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

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

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

Art. 25. Deverá ser nomeado um Gestor de Segurança da Informação, no âmbito de cada Tribunal Eleitoral, com as seguintes responsabilidades:

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

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

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

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

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

Art. 26. 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 VI

DAS COMPETÊNCIAS DAS UNIDADES

Art. 27. Compete à Presidência:

I - apoiar a aplicação das ações estabelecidas nesta PSI;

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

a) do Gestor da Comissão de Segurança da Informação, nos termos do art. 22;

b) do Gestor de Segurança da Informação e seu substituto, nos termos do art. 25, parágrafo único;

c) de integrantes da ETIR, nos termos do art. 26.

Art. 28. Compete ao Diretor-Geral da Secretaria do Tribunal:

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

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

III - apoiar a aplicação das ações estabelecidas nesta PSI;

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

Art. 29. Compete à Secretaria de Tecnologia da Informação:

I - apoiar a implementação desta PSI;

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

III - garantir que os níveis de acesso lógico concedidos aos usuários estejam adequados aos propósitos do negócio e condizentes com as normas vigentes de segurança da informação;

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

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

Art. 30. Compete à Secretaria de Administração:

I - implantar controles nos ambientes físicos, visando prevenir danos, furtos, roubos, interferência e acesso não autorizado às instalações e ao patrimônio da Justiça Eleitoral;

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;

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

IV - 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;

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

Parágrafo único. Havendo, no Tribunal, unidade específica responsável pela segurança física dos ambientes, as atribuições indicadas nos incisos I e II serão de sua competência.

Art. 31. Compete à unidade 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 às demais unidades do Tribunal, 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;

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

Art. 32. Compete à Assessoria de Comunicação ou unidade responsável por essa atividade, 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. 33. Compete à Corregedoria Eleitoral:

I - empreender medidas e expedir normas para adequar as práticas cartorárias a esta PSI;

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

Art. 34. Compete à unidade de Controle Interno e Auditoria:

I - incluir no escopo do Plano Anual de Auditoria e Conformidade, nos termos estabelecidos no art. 17, a análise do cumprimento desta PSI, seus regulamentos e demais normativos de segurança vigentes;

II - realizar auditorias conforme Plano Anual de Auditoria e Conformidade;

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

Art. 35. 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. 36. 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. 37. Compete aos 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 - executar as orientações técnicas e os procedimentos estabelecidos pela Comissão de Segurança da Informação;

VI - gerenciar os ativos sob sua responsabilidade.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 38. Os casos omissos desta PSI serão resolvidos pelas Comissões de Segurança da Informação dos Tribunais Eleitorais.

Art. 39. Esta PSI é obrigatória a todos os Tribunais Eleitorais, os quais terão até 31 de dezembro de 2017 para se adaptarem às regras previstas nesta resolução.

Art. 40. Esta PSI e demais normas, procedimentos, planos e/ou processos deverão ser publicados na Intranet de cada Tribunal pela respectiva Comissão de Segurança da Informação.

Art. 41. 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.

Art. 42. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo Tribunal devem observar, no que couber, o constante desta PSI.

Art. 43. Esta resolução entra em vigor na data de sua publicação, revogada a Resolução-TSE nº 22.780, de 24 de abril de 2008.

Brasília, 19 de dezembro de 2016.

MINISTRO GILMAR MENDES — PRESIDENTE E RELATOR

MINISTRA ROSA WEBER

MINISTRO HERMAN BENJAMIN

MINISTRO NAPOLEÃO NUNES MAIA FILHO

MINISTRO HENRIQUE NEVES DA SILVA

MINISTRA LUCIANA LÓSSIO

RELATÓRIO

O SENHOR MINISTRO GILMAR MENDES: Senhores Ministros, o Diretor-Geral da Secretaria do Tribunal encaminha minuta de resolução proposta pelo Grupo de Trabalho de Governança de Tecnologia da Informação, aprovada pela Comissão de Tecnologia da Informação, no sentido de instituir no âmbito desta Justiça especializada a Política de Segurança da Informação (PSI), tendo como princípio norteador a garantia da integridade, da autenticidade, da confidencialidade, da disponibilidade e da irretratabilidade de informação e de processamento (fl. 144).

Nos termos do despacho de fl. 145, determinei fosse o assunto autuado como processo administrativo.

Os autos vieram conclusos em 15.9.2016.

É o relatório.

VOTO

O SENHOR MINISTRO GILMAR MENDES (presidente e relator): Senhores Ministros, submeto à consideração de Vossas Excelências proposta de resolução que dispõe sobre o estabelecimento da Política de Segurança da Informação (PSI) da Justiça Eleitoral.

A proposta foi inicialmente desenvolvida pelo Grupo de Trabalho de Governança de Tecnologia da Informação e aprovada pela Comissão de Tecnologia da Informação da Secretaria de Tecnologia da Informação do TSE, bem como por todos os Secretários de TI da Justiça Eleitoral, segundo consta do Protocolo-TSE nº 13.386/2015.

Conforme se verifica do Procedimento SEI nº 2015.00.000000307-4, o texto foi submetido às seguintes unidades deste Tribunal: Secretaria da Presidência, Secretaria de Administração, Secretaria de

Gestão de Pessoas, Assessoria de Comunicação, Secretaria Judiciária, Secretaria de Controle Interno, Secretaria de Tecnologia da Informação e Corregedoria-Geral Eleitoral. Na mesma linha, os Tribunais Regionais Eleitorais foram consultados quanto à minuta (Ofício-Circular GDG nº 3.726/2015). As sugestões de alteração propostas foram minuciosamente analisadas, tendo sido incorporadas as consideradas pertinentes.

Além disso, conforme consta do Procedimento Administrativo SEI nº 2016.00.000017029-4, a minuta foi aprovada pela Ouvidoria e pela Secretaria de Gestão da Informação, a qual sugeriu a inclusão, entre os considerandos, a Resolução-TSE nº 23.379/2012, que dispõe sobre o Programa de Gestão Documental no âmbito da Justiça Eleitoral, o que foi realizado.

A matéria atualmente está regulamentada neste Tribunal pela Res.-TSE nº 22.780/2008, em relação à qual se propõe sua revogação, por estas razões:

> 4.1 A versão proposta da POSIC, em muito, se baseou na resolução anterior. Assim, trata-se de uma modernização daquela Política onde não houve redução da abrangência, mas a ampliação do escopo anterior e o destaque de alguns elementos, tais como: Gestão de Continuidade de Negócios, Tratamento de Incidentes de Rede, entre outros. Dessa forma, entendo que não se pode manter válida parte daquela resolução, uma vez que toda ela está contida na atual.
>
> 4.2 Não revogar a Resolução nº 22.780 pode causar conflitos de conceitos e de competências, uma vez que em seu Art. 9º é estabelecida a obrigação de que seja constituída uma Comissão de Segurança da Informação composta por representantes da Diretoria-Geral, da Corregedoria, da Secretaria de Tecnologia da Informação e da Secretaria de Gestão de Pessoas, enquanto a minuta proposta estabelece, em seu Art. 19, que a Comissão será composta por representantes da Presidência, da Diretoria-Geral, da Corregedoria e de cada Secretaria, além de atribuir algumas competências a uma nova equipe, a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), não prevista na resolução anterior.
>
> (Informação nº 17/2015 ASPLAN/STI, Procedimento SEI nº 2015.00.000000307-4).

Instada a se manifestar sobre eventual impacto com o disposto na Res.-TSE nº 23.435/2015, que regulamenta, no âmbito deste Tribunal, a

aplicação da Lei nº 12.527/2011, que dispõe sobre o acesso à informação, a Assessoria Jurídica registra:

> Da análise da Resolução nº 23.435, não se identifica conflito, sob o aspecto jurídico, com a proposta de implementação da POSIC, no tocante à disponibilidade da informação, porquanto aquela norma, especial, trata especificamente do acesso à informação, sob a ótica da Lei que disciplina o tema.
>
> (Parecer ASJUR nº 31/2015, Procedimento SEI nº 2015.00.000000307-4)

As regras constantes da minuta estão alinhadas com o Decreto nº 3.505/2000, que institui a PSI nos órgãos e entidades da Administração Pública Federal, e com a Norma Complementar nº 03/2015 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República que fixa diretrizes para a elaboração da referida Política.

Tendo em vista o disposto no art. 11 da Lei nº 8.868/1994[1] proponho que a PSI seja obrigatória a todos os Tribunais Eleitorais, os quais terão até 31 de dezembro de 2017 para se adaptarem às novas regras.

Ante o exposto, considerando as manifestações das áreas técnicas e tendo em vista que a adoção da PSI em toda a Justiça Eleitoral acarretará o aprimoramento da política de governança de TI, bem como trará uniformidade de procedimentos nos Tribunais Eleitorais, **submeto** aos pares a minuta de resolução que institui a PSI no âmbito desta Justiça especializada.

---

[1] Art. 11. As atividades a serem desenvolvidas nas áreas de planejamento de eleições, informática, recursos humanos, orçamento, administração financeira, controle interno de material e patrimônio serão organizadas sob a forma de sistemas, cujos órgãos centrais serão as respectivas unidades do Tribunal Superior Eleitoral.

§ 1º As disposições constantes do caput deste artigo aplicam-se a outras atividades auxiliares comuns que necessitem de coordenação central na Justiça Eleitoral.

§ 2º Os serviços incumbidos das atividades de que trata este artigo são considerados integrados ao respectivo sistema e ficam, conseqüentemente, sujeitos à orientação normativa, supervisão técnica e à fiscalização específica do órgão central do sistema, sem prejuízo da subordinação hierárquica aos dirigentes dos órgãos em cuja estrutura administrativa estiverem integrados.