Poder Judiciário
TRIBUNAL REGIONAL ELEITORAL DE SERGIPE

RESOLUÇÃO N. 10/2019

INSTRUÇÃO PJe 0600050-11.2019.6.25.0000
Interessado: Tribunal Regional Eleitoral de Sergipe – TRE/SE

Dispõe sobre a Política de Segurança da Informação (PSI) da Justiça Eleitoral de Sergipe, revogando a Resolução TRE-SE nº 180, de 17 de dezembro de 2013.

O TRIBUNAL REGIONAL ELEITORAL DE SERGIPE, no uso das atribuições legais e em conformidade com o disposto no artigo 96, I, a e b, da Constituição Federal, e no artigo 30, XVI, do Código Eleitoral, resolve expedir as seguintes instruções:

CONSIDERANDO o disposto no artigo 27 da Resolução TSE n° 23.501 de 19 de dezembro de 2016 - Política de Segurança da Informação da Justiça Eleitoral (PSI) que estabelece a competência da Presidência de cada Tribunal integrante da Justiça Eleitoral quanto ao apoio à aplicação das ações estabelecidas na Política de Segurança da Informação e normas correlatas;

CONSIDERANDO a edição da Lei n° 12.527, de 18 de novembro de 2011, sobre o acesso à informação previsto na Constituição Federal;

CONSIDERANDO que o Tribunal produz e custódia informações no exercício de suas competências e que eventual sigilo dessas informações deve ser resguardado;

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 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;

RESOLVE:

CAPÍTULO I
DOS CONCEITOS E DEFINIÇÕES

Art. 1° Instituir, no âmbito do Tribunal Regional Eleitoral de Sergipe, as diretrizes da Política de Segurança da Informação da Justiça Eleitoral (PSI), de acordo como estabelecido através da Resolução TSE n° 23.501/2016.

Art. 2° Para os efeitos desta Resolução e em consonância com a PSI da Justiça Eleitoral, 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 JustiçaEleitoral;

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. **custodiante**: qualquer pessoa física ou jurídica, interna ou externa, que detém a posse, mesmo que transitória, de informação produzida ou recebida pelo Tribunal;

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

XIV. **disponibilidade**: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada;

XV. **gerenciamento de riscos**: atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos, incluindo a análise e avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos;

XVI. **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;

XVII. **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;

XVIII. **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;

XIX. **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;

XX. **integridade**: propriedade que garante que a informação mantém todas as características originais estabelecidas pelo proprietário;

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

XXII. **Programa de Gestão de Segurança da Informação (PGSI)**: grupo de projetos relacionados à segurança da informação, gerenciados de modo coordenado para obtenção de benefícios e controle que não estariam disponíveis se eles fossem gerenciados individualmente;

XXIII. **quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no

comprometimento da segurança da informação;

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

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

XXVI. **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;

XXVII. **risco**: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças com impacto negativo no negócio da organização;

XXVIII. **segurança da informação**: abrange aspectos físicos, tecnológicos e humanos da organização e se orienta pelos princípios da autenticidade, confidencialidade, integridade, disponibilidade e irretratabilidade da informação, entre outras propriedades;

XXIX. **Sistema de Gestão de Segurança da Informação (SGSI)**: a parte do sistema de gestão global, baseada na abordagem de riscos do negócio para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação;

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

XXXI. **usuário:** aquele que utiliza de forma autorizada recursos inerentes às atividades precípuas da Justiça Eleitoral;

XXXII. **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 do Tribunal Regional Eleitoral de Sergipe:

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 A PSI se aplica aos 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 deste Tribunal.

Parágrafo único. Os destinatários da 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, em sendo necessário, normas, procedimentos, planos e/ou processos, no que tange às Seções a seguir elencadas.

Parágrafo único. Conforme necessidade e conveniência, poderão ser criados normativos sobre outros temas.

Seção I
Da Gestão de Ativos

Art. 7º Os ativos de informação e de processamento deste Tribunal 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 por este Tribunal 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 terceiros, bem como para veicular opiniões político-partidárias, ficando sujeitos os responsáveis às penas legais.

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 da PSI.

§ 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 pela STI Processo de Gestão de Riscos de Ativos de Informação e de Processamento do TRE, 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, preferencialmente a cada 6 meses.

Seção IV
Da Gestão da Continuidade de Negócios

Art. 14. Deverá ser elaborado pela STI 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, preferencialmente a cada 12 meses.

Seção V
Do Tratamento de Incidentes de Rede

Art. 15. Deverá ser elaborado pela STI Processo de Tratamento e Resposta a Incidentes em Redes de Computadores, visando a 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;

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 da 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 24 meses 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 do Tribunal Regional Eleitoral de Sergipe deverá contemplar atividades específicas que garantam maior segurança para os sistemas utilizados, de forma a preservar o ambiente tecnológico e 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 informação classificada em qualquer grau de sigilo, produzida, armazenada ou transmitida pelo Tribunal, em parte ou totalmente e por qualquer meio eletrônico,

deverá ser protegida com recurso criptográfico.

Parágrafo único. A falta de proteção criptográfica poderá ocorrer quando justificada e aprovada pelo Comitê 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:

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

2. **organização:** refere-se ao armazenamento, arquivamento e controle da informação;

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

4. **destinação:** 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. O Comitê de Segurança da Informação (CSI) do TRE/SE será subordinado à Presidência do Tribunal e terá a seguinte composição:

I. o Diretor-Geral do Tribunal Regional Eleitoral de Sergipe e um suplente;

II. um representante da Presidência e um suplente;

III. um representante da Corregedoria e um suplente;

IV. dois representantes da Secretaria de Tecnologia da Informação e suplentes;

V. um representante da Secretaria de Administração e Orçamento e um suplente;

VI. um representante da Secretaria de Gestão de Pessoas e um suplente;

VII. um representante da Secretaria Judiciária e um suplente;

VIII. um representante da Assessoria de Imprensa e Comunicação Social e um suplente.

§ 1° Os membros de que tratam os incisos II e VIII serão indicados pela Presidência e incorporados ao comitê por intermédio de Portaria específica.

§ 2º Os membros de que trata o inciso III serão indicados pela Corregedoria Regional Eleitoral e incorporados ao comitê por intermédio de Portaria específica.

§ 3° Os membros de que tratam os incisos IV a VII serão indicados pela Diretoria-Geral e incorporados ao comitê por intermédio de Portaria específica.

Art. 23. Compete ao Comitê de Segurança da Informação (CSI):

I. propor melhorias à PSI;

II. propor normas, procedimentos, planos e/ou processos, nos termos do artigo 6º, visando à operacionalização da PSI;

III. promover a divulgação da PSI e normativos, bem como de ações para disseminar a cultura em segurança da informação;

IV. propor estratégias para a implantação da PSI;

V. propor ações visando à fiscalização da aplicação das normas e da PSI;

VI. propor recursos necessários à implementação das ações da PSI;

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. A Comissão Técnica de Segurança da Informação (CTSI) será subordinada à Secretaria de Tecnologia da Informação e terá a seguinte composição:

I. o Coordenador de Infraestrutura (COINF) que atuará como presidente;

II. o Coordenador de Sistemas de Informação da STI (COSIS);

III. o Chefe da Seção de Suporte Operacional da STI (SESOP);

IV. o Chefe da Seção de Apoio ao Usuário da STI (SEAPU);

V. um representante da Assessoria de Planejamento da STI (ASPLAN-STI).

Parágrafo único. Os membros da Comissão de que trata este artigo serão designados por intermédio de Portaria específica.

Art. 25. Compete à Comissão Técnica de Segurança da Informação (CTSI):

I. auxiliar tecnicamente o CSI;

II. manter contato permanente e estreito com grupos de interesses especiais ou outros fóruns especializados de segurança da informação e associações profissionais, como forma de ampliar o conhecimento sobre as melhores práticas e se manter atualizado com as informações relevantes sobre segurança da informação, assegurando que o entendimento do ambiente esteja atual e completo;

III. elaborar metodologia para suportar o SGSI, na qual serão detalhadas as tarefas a serem realizadas, os papéis dos responsáveis pela sua execução e suas respectivas atribuições, bem como os artefatos a serem gerados em cada fase do processo.

Art. 26. Deverá ser nomeado um Gestor de Segurança da Informação com as seguintes responsabilidades:

I. propor normas relativas à segurança da informação ao CSI;

II. propor iniciativas para aumentar o nível da segurança da informação ao CSI, 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 pelo CSI;

V. promover a cultura de segurança da informação;

VI. acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

VII. atuar junto aos usuários finais para solução de problemas que coloquem em risco a 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. 27. Deverá ser instituída ETIR, conforme modelo proposto pelo CSI e aprovado

pela Diretoria-Geral 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.

CAPÍTULO VI
DAS COMPETÊNCIAS DAS UNIDADES

Art. 28. Compete à Presidência:

I. apoiar a aplicação das ações estabelecidas na PSI;

II. nomear ou delegar à Diretoria-Geral a nomeação:

a) do Gestor do Comitê de Segurança da Informação dentre os componentes do CSI especificados no artigo 22, preferencialmente os relativos ao inciso IV;

b) do Gestor de Segurança da Informação e seu substituto, nos termos do artigo 26, parágrafo único;

c) de integrantes da ETIR, nos termos do artigo 27.

Art. 29. Compete à Diretoria-Geral do Tribunal:

I. aprovar normas, procedimentos, planos e/ou processos que lhe forem submetidos pelo CSI;

II. submeter à Presidência as propostas que extrapolem sua alçada;

III. apoiar a aplicação das ações estabelecidas na PSI;

IV. viabilizar recursos com vistas às ações constantes da PSI, inclusive a exequibilidade do Plano de Continuidade de Negócios do Tribunal, abrangendo sua manutenção, treinamento e testes periódicos.

Art. 30. Compete à Secretaria de Tecnologia da Informação:

I. apoiar a implementação da PSI;

II. prover os ativos de processamento necessários ao cumprimento da 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 pelo CSI.

Art. 31. Compete à Secretaria de Administração, Orçamento e Finanças:

I. implantar controles nos ambientes físicos, visando a 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. 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;

IV. executar as orientações técnicas e procedimentos estabelecidos pelo CSI.

Art. 32. Compete à Secretaria de Gestão de Pessoas:

I. apoiar o CSI 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 da lotação ou desligamento de pessoal e comunicar às demais unidades do Tribunal com vistas à permissão ou remoção dos acessos às informações da Justiça Eleitoral;

III. promover a capacitação dos servidores que integram a estrutura de gestão da segurança da informação;

IV. executar as orientações técnicas e os procedimentos estabelecidos pelo CSI.

Art. 33. Compete à Assessoria de Imprensa e Comunicação Social:

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

II. divulgar a PSI;

III. executar as orientações técnicas e os procedimentos estabelecidos pelo CSI.

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

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

II. realizar auditorias conforme o Plano Anual de Auditoria e Conformidade;

III. executar as orientações técnicas e procedimentos estabelecidos pelo CSI.

Art. 35. Compete à Coordenadoria de Gestão da Informação:

I. regulamentar e coordenar o processo de classificação da informação estabelecido pelo Tribunal;

II. executar as orientações técnicas e os procedimentos estabelecidos.

Art. 36. Compete às Zonas Eleitorais:

I. apoiar o CSI 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 pelo CSI.

Art. 37. Compete aos usuários:

I. responder por todas as atividades executadas com o uso de sua identificação;

II. ter pleno conhecimento da 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 pelo CSI;

VI. gerenciar os ativos sob sua responsabilidade.

CAPÍTULO VII
DAS DISPOSIÇÕES FINAIS

Art. 38. Os casos omissos da PSI serão resolvidos pelo Comitê de Segurança da Informação.

Art. 39. A PSI e demais normas, procedimentos, planos e/ou processos deverão ser publicados na Intranet pelo CSI.

Art. 40. O descumprimento da PSI será objeto de apuração pela Presidência ou Corregedoria, conforme o caso, 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. 41. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo Tribunal devem observar, no que couber, o constante da PSI.

Art. 42. Esta Resolução entra em vigor na data de sua publicação, revogando as disposições em contrário.

Sala de Sessões do Tribunal Regional Eleitoral de Sergipe, aos vinte e um dias do mês de março do ano de dois mil e dezenove.

Des. JOSÉ DOS ANJOS
Presidente

Des. DIÓGENES BARRETO
Vice-Presidente e Corregedor Regional Eleitoral

Juiz MARCOS ANTÔNIO GARAPA DE CARVALHO

Juíza ÁUREA CORUMBA DE SANTANA

Juiz HÉLIO DE FIGUEIREDO MESQUITA NETO

Juiz JOABY GOMES FERREIRA

Juíza SANDRA REGINA CÂMARA CONCEIÇÃO