RESOLUÇÃO Nº 5.430

PROCESSO ADMINISTRATIVO Nº 0600067-87.2018.6.14.0000 – BELÉM-PA
INTERESSADO: TRIBUNAL REGIONAL ELEITORAL DO PARÁ
RELATORA: DESEMBARGADORA CÉLIA REGINA DE LIMA PINHEIRO

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

A PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO PARÁ, no uso de suas atribuições legais e regimentais,

CONSIDERANDO que as informações no Tribunal Regional Eleitoral do Pará são armazenadas de diferentes formas, veiculadas em diferentes meios físicos e eletrônicos e são, portanto, vulneráveis a incidentes como desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furtos;

CONSIDERANDO a RESOLUÇÃO CNJ Nº 211 de 15 de dezembro de 2015, que dispõe sobre as diretrizes gerais para a implantação da Gestão de Segurança da Informação no Poder Judiciário;

CONSIDERANDO a RESOLUÇÃO TSE Nº 23.501, de 19 de dezembro de 2016, que dispõe sobre de diretrizes gerais para a implantação da Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a necessidade de implantação da estrutura normativa, que reflita as diretrizes, deveres e responsabilidades referentes à Segurança da Informação, objetivando garantir a integridade, confidencialidade, autenticidade, irretratabilidade e disponibilidade das informações;

CONSIDERANDO a importância da Segurança da Informação para o processo judicial eletrônico - PJe;

/ld

RESOLVE:

Art. 1º Estabelecer a Política de Segurança da Informação e Comunicação do Tribunal Regional Eleitoral do Pará.

CAPÍTULO I
DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para efeitos desta Resolução, 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 e meio 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. segurança da informação: preservação da autenticidade, da confidencialidade, da integridade e da disponibilidade da e do não-repúdio da informação;

V. ativo de informação: patrimônio composto por todos os dados e informações gerados, adquiridos, utilizados ou armazenados pela Justiça Eleitoral;

VI. 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;

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

VIII. integridade: garantia de que a informação esteja inalterada desde sua geração ou alteração autorizada;

IX. disponibilidade: garantia de que a informação esteja sempre disponível às pessoas autorizadas;

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

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

XII. recurso de tecnologia da informação e comunicação (TIC): qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, ou as instalações físicas que os abriguem;

XIII. usuário: qualquer pessoa que utilize sistemas e/ou demais recursos de TIC da instituição;

XIV. plano de continuidade do negócio: conjunto de ações de prevenção e procedimentos de recuperação a serem exercitados e implementados, objetivando proteger os processos críticos de trabalho contra efeitos de falhas de equipamentos, acidentes, ações intencionais ou desastres naturais significativos, assegurando a integridade e disponibilidade das informações;

XV. gestão de segurança da informação: ações e métodos de gestão de riscos, gestão de continuidade de negócios, tratamento de incidentes, conformidade, segurança física, segurança lógica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando à tecnologia da informação;

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. proprietário da informação: pessoa ou setor que produz a informação, capaz de estimar em que nível de criticidade ela se enquadra;

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

XX. 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 poderem compartilhar recursos físicos e lógicos, sendo que estes podem ser do tipo dados, impressoras, mensagens (e-mails), entre outros;

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

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

CAPÍTULO II
DOS PRINCÍPIOS

Art. 3º Esta PSI alinha-se às estratégias e à Política de Segurança da Informação da Justiça Eleitoral e à Resolução CNJ Nº 211/2015 (ENTIC-JUD) 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:

I. instituir diretrizes estratégicas, responsabilidades e competências objetivando a estruturação das normas de segurança da informação no âmbito do Tribunal Regional Eleitoral do Pará;

II. promover e viabilizar ações necessárias à implantação e manutenção da segurança da informação;

III. prevenir, mitigar e/ou combater atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos de informação e a imagem da instituição;

IV. promover a conscientização e a capacitação usuários de recursos de TIC do TRE-PA em segurança da informação através de palestras e seminários.

Art. 5º As disposições desta Política de Segurança da Informação, normas e procedimentos relacionados aplicam-se a todos os magistrados, membros do Ministério Público Eleitoral, servidores efetivos, cedidos e requisitados, ocupantes de cargos em comissão sem vínculo efetivo, estagiários, prestadores de serviço, colaboradores, pensionistas, jurisdicionados, inativos e usuários externos que fazem uso dos ativos de informação e de processamento, no âmbito do Tribunal Regional Eleitoral do Pará.

§ 1º Os destinatários desta PSI, relacionados no caput, são co-responsáveis pela segurança da informação, de acordo com os preceitos estabelecidos nesta Resolução e normas complementares.

§ 2º As disposições desta PSI são válidas para outras pessoas que se encontrem a serviço ou em visita ao Tribunal Regional Eleitoral do Pará, autorizadas a utilizar temporariamente os recursos de tecnologia da informação e comunicações da instituição.

Art. 6º O uso adequado dos recursos de tecnologia da informação e comunicação visa garantir a continuidade da prestação jurisdicional deste Tribunal.

§ 1º Os recursos de tecnologia da informação e comunicação, pertencentes ao Tribunal Regional Eleitoral do Pará e que estão disponíveis para os usuários relacionados no art 5° devem ser utilizados em atividades estritamente relacionadas às funções institucionais.

§ 2º Os recursos de tecnologia da informação e comunicação, utilizados pelos usuários associados ao art 5°, serão monitorados pela instituição.

Art. 7º As informações geradas no âmbito deste Tribunal são de sua propriedade, independente da forma de apresentação ou armazenamento. Assim, essas informações devem ser adequadamente protegidas e utilizadas exclusivamente para fins relacionados às atividades desenvolvidas neste Tribunal.

§ 1º Toda informação gerada no Tribunal deverá ser classificada em termos de seu valor, requisitos legais, sensibilidade, criticidade e necessidade de compartilhamento.

§ 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.

CAPÍTULO IV
DA ESTRUTURA NORMATIVA

Art. 8º O arcabouço normativo da Segurança da Informação no Tribunal Regional Eleitoral do Pará será estabelecido e organizado conforme demonstrado nas estruturas a seguir:

I. Nível Estratégico:

- Política de Segurança da Informação, expedida pela Comissão de Segurança da Informação, constituída pelo presente documento, o qual define as diretrizes fundamentais e princípios basilares incorporados pela instituição à sua gestão, de acordo com a visão definida pelo Planejamento Estratégico da Instituição e segundo as orientações da PSI da Justiça Eleitoral. Este documento serve como base para que possam ser criadas normas detalhadas, complementares à estrutura da Segurança Informação, com definições de direitos e responsabilidades sobre os ativos e recursos de TIC;

II. Nível tático:

• Normas complementares sobre Segurança da Informação, expedidas pela Comissão de Segurança da Informação, integrantes à resolução principal (PSI), fundamentadas de acordo com as temáticas e diretrizes estabelecidas na Política de Segurança da Informação. As orientações adicionais estão associadas ao plano tático, cujos controles deverão ser implementados para alcance da estratégia de Segurança da Informação da instituição. As referidas normas devem abarcar, no mínimo:

a) Gestão de ativos de TIC;

b) Gestão de identidade e acesso lógico às informações;

c) Utilização de recursos de TIC (Estações de trabalho, Internet, correio eletrônico, softwares, certificado digitais, armazenamento lógico, rede VPN, dentre outros).

d) Geração e restauração de cópias de segurança (backup);

e) Tratamento e classificação da informação;

f) Tratamento de incidentes de redes e instituição de equipes responsáveis por esta atividade;

g) Gestão de Incidentes de Segurança da Informação;

h) Gestão da contingência e continuidade do negócio;

i) Monitoração e auditoria de recursos de TIC;

j) Desenvolvimento de Sistemas Seguros.

I. Nível Operacional:

• Procedimentos de Segurança da Informação desenvolvidos em nível operacional, expedidos pelas unidades técnicas da Secretaria de Tecnologia da Informação, compostos por procedimentos, roteiros técnicos, fluxos de processos, Políticas de Acesso à Rede e Internet, Planos de Cópia de Dados Institucionais, manuais com informações técnicas que instrumentalizam o disposto nas normas referenciadas no plano tático, permitindo a aplicação direta da PSI nas atividades técnicas do Tribunal. O nível operacional deverá ocupar-se dos seguintes documentos, dentre outros:

a) Gestão de Continuidade de Serviços Essenciais de TIC;

b) Políticas de Backup da instituição;

c) Gestão de Incidentes de Segurança em Redes Computacionais;

d) Relatórios de Incidentes de Segurança;

e) Gestão de Riscos de Tecnologia da Informação e Comunicação;

f) Gestão dos processos de desenvolvimento e sustentação de software.

Art. 9º Os documentos integrantes da estrutura normativa da Segurança da Informação deverão ser aprovados e revisados conforme os critérios a seguir:

I. Nível Estratégico

- Tipo de Documento: Resolução
- Nível de aprovação: Tribunal Pleno
- Periodicidade da revisão: bienal

II. Nível Tático

- Tipo de Documento: Instruções Normativas
- Nível de aprovação: Presidência
- Periodicidade da revisão: bienal

III. Nível Operacional

- Tipo de Documento: Portarias e seus anexos
- Nível de aprovação: Diretoria Geral
- Periodicidade da revisão: anual

Art. 10 A Resolução da Política de Segurança da Informação, Instruções Normativas complementares, procedimentos e normas técnicas integrantes da estrutura normativa devem ser divulgadas a todos os magistrados, servidores, estagiários e prestadores de serviços quando de sua posse/admissão, bem como através dos meios oficiais de divulgação interna da instituição e, também, publicadas na Intranet institucional, de maneira que seu conteúdo possa ser consultado a qualquer momento.

CAPÍTULO V
DA ESTRUTURA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Seção I
Da Comissão de Segurança da Informação

Art. 11. Deverá ser constituída a 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 pela unidade que desempenhe essa atividade; observado o mandato de 2 (dois) anos para seus integrantes.

Parágrafo único. A Secretaria de Controle Interno e Auditoria - SCIA não terá membro partícipe na mencionada comissão, cabendo-lhe exercer as prerrogativas de Auditoria Interna sobre a gestão da segurança da informação.

Art. 12. 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;

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 - indicar os integrantes da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

XII - responder pela segurança da informação.

Seção II

Do Gestor de Segurança da Informação e Comunicações

Art. 13. Deverá ser nomeado um Gestor de Segurança da Informação, 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;

Parágrafo único. O Gestor de Segurança da Informação, servidor público efetivo, deverá possuir amplo conhecimento dos processos de negócio do Tribunal e do tema em foco.

Seção III

Da Equipe de Tratamento de Incidente de Redes

Art. 14. Deverá ser instituída a Equipe de Tratamento de Incidente de Redes - ETIR, conforme modelo proposto pela Comissão de Segurança da Informação e aprovado pelo Diretor-Geral da Secretaria do Tribunal.

Art. 15 Compete à ETIR:

I - 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;

II - coordenar, analisar, sugerir e/ou implementar ações apropriadas para remoção de qualquer ativo de informação, objeto ou vulnerabilidade que possa causar prejuízos aos sistemas e redes de computadores ou quebra de segurança;

III - disseminar alertas de vulnerabilidades e outras notificações relacionadas à Segurança da Informação no âmbito do Tribunal;

IV - avaliar e analisar riscos atuais e iminentes, bem como propor ações para sua mitigação; e

V - realizar outras atribuições que lhe forem cometidas pela Comissão de Segurança da Informação.

Parágrafo único - Os membros da ETIR deverão ter perfil técnico adequado às funções de tratamento de incidentes em redes computacionais.

CAPÍTULO VI
DAS VIOLAÇÕES E SANÇÕES

Art.16 São consideradas violações à política, às normas ou aos procedimentos de Segurança da Informação as seguintes situações, não se limitando às mesmas:

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

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

III- Uso de dados, informações ou recursos de TIC para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos

internos e externos, da ética ou de exigências de organismos reguladores da área de atuação da instituição;

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

Art.17 O descumprimento à esta PSI, normas e aos procedimentos de Segurança da Informação expedidos pela CSI, será objeto de apuração pela unidade competente do Tribunal a implantação de meio de sindicância ou processo administrativo disciplinar podendo acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurado(s) ao(s) envolvido(s) o contraditório e a ampla defesa.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS

Art. 18 Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo Tribunal devem observar, no que couber, o constante desta PSI.

Art. 19 Esta PSI e demais normas, procedimentos, planos e/ou processos deverão ser publicados na Intranet do Tribunal Regional Eleitoral do Pará.

Art. 20 As normas, procedimentos relacionadas no Art 8°, incisos II e III, descritos neste Capítulo, deverão ser implementadas até o final do exercício de 2018, a fim de viabilizar a consecução do Plano Estratégico Institucional quanto à gestão da segurança da informação.

Art. 21 A presente Resolução entra em vigor a partir da data de sua publicação.

Art. 22 Revogam-se as disposições em contrário.

Sala das Sessões do Tribunal Regional Eleitoral do Pará.

Belém, 27 de março de 2018.

Desembargadora **CÉLIA REGINA DE LIMA PINHEIRO**
Presidente e Relatora

Desembargador **ROBERTO GONÇALVES DE MOURA**

Juiz Federal **ARTHUR PINHEIRO CHAVES**

Juiz **AMILCAR ROBERTO BEZERRA GUIMARÃES**

Juiz **ÁLVARO JOSÉ NORAT DE VASCONCELOS**

Juíza **LUZIMARA COSTA MOURA**

Dra. **NAYANA FADUL DA SILVA**
Procuradora Regional Eleitoral

PODER JUDICIÁRIO
Tribunal Regional Eleitoral do Pará
SECRETARIA JUDICIÁRIA
CSJD/SAR – Seção de Acórdãos e Resoluções

INSTRUÇÃO Nº 0600067-87.2018.6.14.0000

CERTIDÃO DE PUBLICAÇÃO

CERTIFICO que a **Resolução nº 5.430** foi disponibilizada no Diário de Justiça Eletrônico nº **055**, no dia 2.4.2018, páginas **3-6** e será considerada publicada no dia **3.4.2018,** primeiro dia útil seguinte ao da respectiva disponibilização no DJE.

Belém, dois de abril do ano de dois mil e dezoito.

Elaine de Jesus Santana Machado
Chefe da Sessão de Acórdãos e Resoluções