TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
COMISSÃO PERMANENTE DE SEGURANÇA DA INFORMAÇÃO

ATA DE REUNIÃO N. 001/2019

I. Identificação da Reunião

Data	Horário		Local	Coordenador
	Início	Término		
09.08.19	09h00	10h20	Sala de videoconferência	Marcos Flávio Nascimento Maia

II. Objetivo

Reunião da CPSI para tratar dos seguintes assuntos:

1. Proposta de Política de Segurança da Informação do TRE/RN;
2. Proposta de mapeamento do processo de elaboração, acompanhamento e revisão da Política;
3. Plano de Ação da CPSI;
4. Indicador PEJERN IA-37 - Índice de gestão da segurança da informação (Garantir a evolução do sistema de gestão de segurança da informação, por meio da implantação dos controles previstos na norma ABNT ISO 27001/27002)

III. Participantes

Nome	Lotação	Assinatura
Marcos Flávio Nascimento Maia - Presidente da CPSI	STIC	
Virgínia Coelli Rocha da Cruz	ASCOM/ PRES	
Rafael Fonseca Alves - Suplente	NSPRES/ PRES	
Emídia Luiza Dantas Alves França (Suplente)	AJCRE/CRE	
Fernanda Araújo Cruz Barbosa	GABDG	
Liliane Priscila Bezerra da Silva Miranda Gomes	CGI/SJ	
Roberto Silva do Nascimento (Suplente)	SENG/CAP/SAO	
Fláuber Kley de Araújo Cândido	SRF/COPES/SGP	
Carlos Magno do Rozário Câmara	CIT/STIC	
Daniel César Gurgel Coelho Ponte	SRI/CIT/ STIC	
Carlos André de Azevedo Moura (Suplente)	SSP/CIT/ STIC	
Carlos Alberto Narciso Fernandes	SBDS/CS/ STIC	
Helder Jean Brito da Silva	Representante do ETIR	

IV. Discussão da Pauta

Nº	Descrição/Decisão	Responsável
01	Proposta de Política de Segurança da Informação do TRE/RN • Foi apresentada a proposta de minuta de Resolução para instituir a PSI no âmbito do TRE/RN, alinhada à Resolução TSE 23.501/2016 e às Diretrizes do CNJ. • Foi proposto por Liliane a inclusão das determinação da Resolução TRE/RN n. 15/2016, sobre o Acesso à Informação, além da Resolução TRE/RN 22/2016, que trata da gestão documental. • Foi verificado que é necessário acrescentar competência à Presidência no que diz respeito à aprovação de normas que são de sua alçada. • Devem ser ajustadas as nomenclaturas que porventura contenham as Unidades relacionadas à Secretaria de Administração e Orçamento que foi reestruturada esta semana. • Foram ajustadas as competências do NSPRES, para inserir a competência de execução dos procedimentos técnicos. • Após as considerações feitas em reunião, a minuta foi aprovada por todos os presentes, devendo ser encaminhada para apreciação superior (Anexo 1 desta Ata).	Marcos Maia
02	Proposta de mapeamento do processo de elaboração, acompanhamento e revisão da Política • Foi apresentado o fluxo do processo de Elaboração, Acompanhamento e Revisão da Política de Segurança da Informação • Necessário ajustar a etapa da publicação, visto que é feita diretamente pela Presidência (ato formal, no Diário da Justiça Eletrônico) e esclarecer a etapa de divulgação. • O fluxo foi devidamente aprovado pela Comissão, restando necessário a elaboração do manual com detalhamento das atividades, devendo ser submetido para aprovação (Anexo 2 desta Ata).	Marcos Maia
03	Plano de Ação da CPSI • O Plano de Ação elaborado foi proposto à Comissão. • Foi informado por Liliane que as normas de classificação da informação e o mapeamento do processo já foram elaborados pela CPAD e serão encaminhadas para o e-mail da comissão. • O Plano foi aprovado pelos presentes, com as atividades e datas propostas, conforme Anexo 3 desta Ata. • Ficou agendada nova reunião para o dia 22.08.2019, às 13h30, para aprovar as minutas das normas complementares	Marcos Maia
04	Indicador PEJERN IA-37 - Índice de gestão da segurança da informação (Garantir a evolução do sistema de gestão de segurança da informação, por meio da implantação dos controles previstos na norma ABNT ISO 27001/27002) • Ficou agendada reunião para o dia 05.09.2019, às 13h30, para consolidar os responsáveis por executar os itens de controle da ABNT ISO 27001/27002, bem como, medir quais os controles já são atendidos pelo TRE/RN.	Marcos Maia

V. Pendências Identificadas

Nº	Pendências	Responsável	Data limite
01	Encaminhar Memorando com minuta da Política de Segurança da Informação para apreciação	Marcos Maia	09.08.2019
02	Elaborar manual do mapeamento do processo de Elaboração, Acompanhamento e Revisão da PSI	Marcos Maia	16.08.2019
03	Encaminhar Memorando com minuta da Portaria de institui o processo de Elaboração, Acompanhamento e Revisão da PSI	Marcos Maia	16.08.2019
04	Envio de e-mail com as normas levantadas pela CPAD e o mapeamento do processo de classificação	Liliane	13.08.2019
05	Reunião para aprovação de normas complementares	Marcos Maia	22.08.2019
06	Reunião para medição do IA37	Marcos Maia	05.09.2019

V. Fechamento da Ata

Data	Nome do relator	Assinatura
09.08.19	Jussara de Gois Borba Melo Diniz	

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE

Resolução n. XXX/2019

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

O TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a Resolução nº 211, de 15 de dezembro de 2015, do Conselho Nacional de Justiça, que, em seu art. 9º, determina que cada órgão deverá elaborar e aplicar política, gestão e processo de segurança da informação a serem desenvolvidos em todos os níveis da instituição;

CONSIDERANDO as Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário de 2012, elaboradas pelo Conselho Nacional de Justiça;

CONSIDERANDO a Resolução nº 23.501, de 19 de dezembro de 2016, do Tribunal Superior Eleitoral, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

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;

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

CONSIDERANDO a Lei Nº 12.527, de 18 de Novembro de 2011, que versa sobre o acesso à informação previsto na Constituição Federal e a Resolução TRE/RN nº 15/2016, que regulamenta a sua aplicação, no âmbito do TRE/RN;

CONSIDERANDO a Resolução TRE/RN nº 22/2016, que dispõe sobre as diretrizes para a implantação do Programa de Gestão Ambiental no âmbito da Justiça Eleitoral do Rio Grande do Norte;

CONSIDERANDO a necessidade de implantação da estrutura normativa, que reflita as diretrizes, deveres e responsabilidades referentes à Segurança da Informação;

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 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 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;

RESOLVE:

Art. 1º Fica regulamentada, nos termos desta Resolução, a Política de Segurança da Informação (PSI), no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte.

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, por meio da adoção de procedimentos e mecanismos, que visam a eliminação ou redução da ocorrência de modificações não autorizadas, bem como garantam a disponibilidade de recursos e sistemas críticos para a continuidade dos negócios do TRE-RN, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores praticas de Segurança da Informação e Comunicação.

Capítulo I
DAS DEFINIÇÕES E CONCEITOS TÉCNICOS

Art. 2º Para 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 - 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 - disponibilidade: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada;
XVII - documento: unidade de registro de informações, qualquer que seja o formato ou o suporte;
XVIII - 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;
XIX - gestor de processo: responsável por acompanhar e controlar o desempenho de um processo, a fim de garantir seus resultados;
XX - 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;
XXI - 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;
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 - proprietário da informação: pessoa ou setor que produz a informação, capaz de estimar em que nível de criticidade ela se enquadra;
XXVII - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;
XXVIII - recurso: além da própria informação, é todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;
XXIX - recurso criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;
XXX - 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;
XXI - risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;
XXXII - 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;
XXXIII - tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;
XXXIV - 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;
XXXV - usuário interno: qualquer pessoa física que faça uso de informações e
exerça atividade na Justiça Eleitoral do Rio de Grande do Norte, ainda que temporariamente, com ou sem remuneração;

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

Capítulo II
DOS PRINCÍPIOS

Art. 3° Esta PSI alinha-se às estratégias e à Política de Segurança da Informação da Justiça Eleitoral, instituída através da Resolução TSE n.° 23.501, de 19 de dezembro de 2016, além da Resolução CNJ n.° 211/2015 (ENTIC-JUD).

Art. 4° As ações relacionadas com a Segurança da Informação no TRE-RN são norteadas pelos seguintes princípios, assim definidos:

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: garantia que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
III - disponibilidade: garantia de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade autorizada;
IV - autenticidade: garantia de que a informação foi produzida, enviada, modificada ou destruída dentro dos preceitos legais e normativos, por pessoa física, ou por sistema, órgão ou entidade autorizada;
V - irretratabilidade (ou não-repúdio): garantia de que a autoria da informação não pode ser negada em uma alteração anteriormente feita, por pessoa física, ou por sistema, órgão ou entidade autorizada;
VI - conformidade – garantia de que a informação produzida, enviada, modificada ou destruída obedece às normas, leis, estatutos, regulamentações ou obrigações contratuais, requisitos legais e quaisquer requisitos de segurança da informação.

Capítulo III
DO ESCOPO

Art. 5° São objetivos desta PSI:

I - instituir diretrizes estratégicas, responsabilidades e competências visando à estruturação das normas de segurança da informação no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte;
II - promover e viabilizar ações necessárias à implementação e à 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 dos usuários em segurança da informação.

Art. 6° 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 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 do Rio Grande do Norte.

§1° Os destinatários desta PSI, relacionados no *caput*, são corresponsáveis pela segurança da informação, de acordo com os preceitos estabelecidos nesta resolução.

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

Art. 7° O uso adequado dos recursos de tecnologia da infomação e comunicação visa garantir a continuidade da prestação jurisdicional deste Tribunal.

§1° Os recursos de tecnologia da informação e comunicação, pertencentes ao Tribunal Regional Eleitoral do Rio Grande do Norte e que estão disponíveis para os usuários relacionados no art. 6° devem ser utilizados em atividades estritamente relacionadas às funções institucionais.

Art. 8° 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 os fins relacionados às atividades desenvolvidas neste Tribunal.

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

§2° 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. 9° A estrutura normativa da segurança da informação, no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte, será estabelecido e organizado conforme demonstrado a seguir:

I - Nível Estratégico: Política 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.

II - Nível Tático: Normas Complementares sobre Segurança da Informação, que contemplam obrigações a serem seguidas de acordo com as diretrizes estabelecidas nesta PSI e devem abarcar, no mínimo:

a. Gestão de Ativos de TIC;
b. Gestão de Identidade e Acesso Lógico às informações;
c. Gestão de Riscos de Ativos de Informação;
d. Gestão de Continuidade de Negócios;
e. Tratamento de Incidentes de Rede;
f. Gestão de Incidentes de Segurança da Informação;
g. Utilização de recursos de TIC (estações de trabalho, serviços de internet, correio eletrônico, softwares, certificados digitais, armazenamento lógico, rede VPN, entre outros);
h. Geração e restauração de cópias de segurança (*backup*);
i. Tratamento e Classificação da Informação; e
j. Desenvolvimento de Sistemas Seguros.

III - Nível Operacional: Procedimentos de Segurança da Informação, que contemplam regras operacionais, roteiros técnicos, fluxos de processos, manuais com informações técnicas que instrumentalizam o disposto nas normas referenciadas no plano tático, de acordo com o disposto nas diretrizes e normas de segurança estabelecidas, permitindo sua utilização nas atividades do órgão, devendo ocupar-se dos seguintes documentos, entre outros:

a. Plano de Continuidade de Serviços Essenciais de TIC;

b. Políticas de *backup* da Instituição;
c. Incidentes de Segurança em Redes Computacionais;
d. Relatórios de Incidentes de Segurança;
e. Gestão de Riscos de Tecnologia da Informação e Comunicação; e
f. Gestão dos processos de desenvolvimento e sustentação de software.

Art. 10° 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: Portarias e seus anexos
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.11 Esta Resolução, normas complementares, procedimentos e normas técnicas integrantes desta estrutura normativa devem ser divulgadas a todos os magistrados, servidores, estagiários e prestadores de serviço quando da 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 Permanente de Segurança da Informação

Art. 12 A Comissão Permanente de Segurança da Informação da Justiça Eleitoral do Rio Grande do Norte (CPSI), subordinada à Presidência do Tribunal, será composta por representantes da Presidência, Corregedoria Regional Eleitoral, Diretoria-Geral, da Assessoria de Comunicação Social e Cerimonial, Secretaria Judiciária, Secretaria de Administração, Orçamento e Finanças, Secretaria de Gestão de Pessoas e Secretaria de Tecnologia da Informação e Comunicação, indicados pelos respectivos titulares das Unidades, tem como competências:

I - propor melhorias à Política de Segurança da Informação da Justiça Eleitoral e a esta própria Política;
II - propor normas, procedimentos, planos e/ou processos, nos termos do art. 9°, 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 deste Tribunal;
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.
XII - analisar criticamente os incidentes de segurança da informação e ações corretivas correlatas;
XIII - promover processos de gerenciamento de riscos, bem como a elaboração e aprovação dos planos de continuidade de negócios;
XIV - definir o plano de auditoria periódica, no âmbito do Tribunal e das Zonas Eleitorais.

§1° A CPSI poderá requisitar temporariamente servidores das unidades do Tribunal para colaborar com as atividades da Comissão.
§2° Sempre que necessário, a CPSI poderá solicitar aos titulares das unidades informações pertinentes à segurança da informação.
§3° O ato de designação da Comissão de Segurança da Informação indicará o seu presidente, o substituto eventual deste e o secretário.

Seção II
Da Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais

Art. 13 A Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais (ETIR) estará vinculada à Secretaria de Tecnologia da Informação e Comunicação e terá como objetivo o cumprimento da missão institucional do TRE/RN, 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.

Seção III
Do Gestor de Segurança da Informação

Art. 14 O Gestor de Segurança da Informação atuará 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;

§ 1° O Gestor de Segurança da Informação deverá ser servidor que detenha amplo conhecimento dos processos de negócio do Tribunal e do tema em foco.
§ 2° O ato de nomeação do Gestor de Segurança da Informação indicará também o seu substituto eventual.
§ 3° 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.
§ 4° Sempre que necessário, o Gestor de Segurança da Informação poderá solicitar aos titulares das unidades informações pertinentes à segurança da informação.

Capítulo VI
DAS COMPETÊNCIAS DAS UNIDADES

Art. 15 Compete à Presidência do TRE-RN:

I - aprovar normas, procedimentos, planos e/ou processos que lhe forem submetidos pela Comissão Permanente de Segurança da Informação;
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 Permanente de Segurança da Informação;
b) do Gestor de Segurança da Informação e seu substituto; e
c) de integrantes da ETIR.

Art. 16 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. 17 Compete à Diretoria-Geral da Secretaria do Tribunal:

I - aprovar normas, procedimentos, planos e/ou processos que lhe forem submetidos pela Comissão Permanente 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. 18 Compete à Secretaria de Tecnologia da Informação e Comunicação, na sua área de atuação:

I - prover o apoio necessário à implementação e compreensão da 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.
VI - subsidiar a Comissão Permanente de Segurança da Informação com o conhecimento de cunho tecnológico, aplicado à execução desta.

Art. 19 Compete à Secretaria de Administração,Orçamento e Finanças:

I - assegurar que os empregados das empresas prestadoras de serviço contratadas conheçam suas atribuições e responsabilidades em relação à segurança da informação;
II - 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;
III - executar as orientações técnicas e procedimentos estabelecidos pela Comissão Permanente de Segurança da Informação.

Art. 20 Compete à Secretaria 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. 21 Compete à Secretaria Judiciária:

I - regulamentar e coordenar o processo de classificação da informação no âmbito do Tribunal;
II - executar as orientações técnicas e os procedimentos estabelecidos pela Comissão Permanente de Segurança da Informação.

Art. 22 Compete ao Núcleo de Segurança da Presidência:

I - implantar controles nos ambientes físicos, visando prevenir danos, furtos, roubos, interferência e acesso não autorizado às instalações e ao patrimônio da Justiça Eleitoral; e
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 ou causados pelo homem;
III - executar as orientações técnicas e os procedimentos estabelecidos pela Comissão Permanente de Segurança da Informação.

Art. 23 Compete à Assessoria de Comunicação Social e Cerimonial em conjunto com a Comissão Permanente 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. 24 Compete à unidade de Auditoria Interna:

I - incluir no escopo do Plano Anual de Auditoria e Conformidade 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 Permanente de Segurança da Informação.

Art. 25 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 Permanente de Segurança da Informação.

Art. 26 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;

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 desta PSI 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 desta PSI;
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 desta PSI;
VII - propor ao Gestor da Segurança da Informação procedimentos visando à regulamentação e operacionalização das diretrizes e normas de segurança apresentadas por esta PSI.

Art. 27 Compete aos usuários:

I - responder por toda atividade executada com o uso de sua identificação;
II - ter pleno conhecimento e seguir esta PSI;
III - reportar tempestivamente ao Gestor de Segurança da Informação ou à CPSI 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;
VII - observar o adequado manuseio e armazenamento de documentos e processos.

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

CAPÍTULO VII
DAS VIOLAÇÕES E SANÇÕES

Art. 28 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 CPSI de quaisquer descumprimentos da política, de normas ou de procedimentos de Segurança da Informação, que porventura um usuário venha a tomar conhecimento.

Art. 29 O descumprimento desta PSI será objeto de apuração pela unidade competente do Tribunal através da implantação de sindicância ou processo administrativo disciplinar podendo acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Capítulo VIII
DAS DISPOSIÇÕES FINAIS

Art. 30 Esta norma e os instrumentos normativos gerados a partir dela deverão ser revisados sempre que se fizerem necessários.

Art. 31 Esta PSI e demais normas, procedimentos, planos e/ou processos deverão ser publicados na Intranet do Tribunal pela Comissão Permanente de Segurança da Informação, garantindo seu amplo conhecimento para adequado usufruto dos benefícios e assunção das responsabilidades sobre os ativos de informação deste Tribunal.

Art. 32 As normas internas do TRE-RN 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 12 (doze) meses contados a partir da data da publicação desta Resolução.

Art. 33 Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres, celebrados pelo Tribunal, devem observar, no que couber, as diretrizes, normas e procedimentos estabelecidos nesta PSI.

Art. 34 Os casos omissos desta PSI serão resolvidos pela Comissão Permanente de Segurança da Informação, juntamente com o Gestor de Segurança da Informação.

Art. 35 A presente Resolução entra em vigor na data de sua publicação.

Sala das Sessões, Natal (RN), XX de agosto de 2019.

Desembargador Glauber Antonio Nunes Rêgo
Presidente

Desembargador Cornélio Alves de Azevedo Neto
Vice-Presidente

Juiz Carlos Wagner Dias Ferreira

Juiz Ricardo Tinoco de Góes

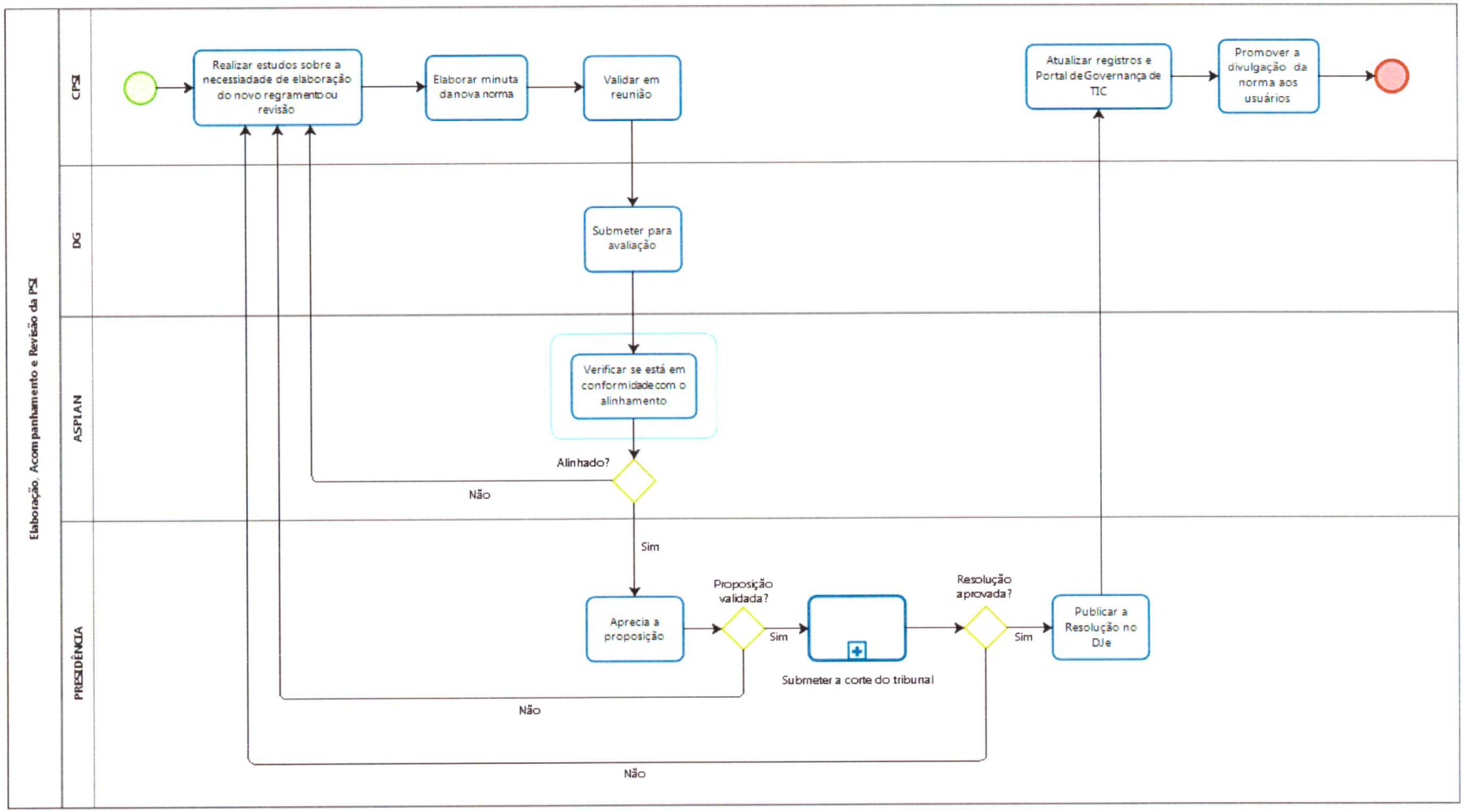
Juiz José Dantas de Paiva

Juíza Adriana Cavalcanti Magalhães Faustino Ferreira

Juiz Wlademir Soares Capistrano

Doutora Cibele Benevides Guedes da Fonseca
Procuradora Regional Eleitoral

Anexo 2 - Ata n.º 01 da CPSI



TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
COMISSÃO DE SEGURANÇA DA INFORMAÇÃO - CPSI
PLANO DE TRABALHO 2019-2020

Código da Ação	Temática	Objetivo Geral	Principais Tópicos	Responsável	Período
1	GESTÃO DA SEGURANÇA DA INFORMAÇÃO	IMPLANTAR A NOVA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO TRE/RN	1.1 Análise e elaboração da nova PSI do TRE/RN	Todos os membros	Agosto/2019
			1.2 Submeter a minuta da Política à aprovação	Todos os membros	Agosto/2019
2		ELABORAÇÃO DOS NORMATIVOS (OU REVISÃO DAS NORMAS E PROCEDIMENTOS EXISTENTES)	2.1 Levantamento de normas de Classificação e Tratamento da Informação	CPAD	Agosto/2019
			2.2 Gestão de Riscos de Ativos de Informação e de Processamento	Todos os membros	Agosto/2019
			2.3 Controle de Acessos e Usos de Recursos de TIC	Todos os membros	Agosto/2019
			2.4 Gestão de Ativos de Informação e de Processamento	STIC	Agosto/2019
			2.5 Gestão de Incidentes de Segurança da Informação	STIC	Agosto/2019
			2.6 Plano de Continuidade de Serviços Essenciais de TIC	STIC	Agosto/2019
3		PROCESSOS DE SEGURANÇA DA INFORMAÇÃO	3.1 Aprovação do Catálogo de Processos de Segurança da Informação	Todos os membros	Agosto/2019
			3.2 Mapeamento do processo de elaboração, acompanhamento e revisão da Política de Segurança da Informação	Todos os membros	Agosto/2019
			3.3 Mapeamento do processo de classificação e tratamento da informação	CPAD	Agosto/2019
			3.4 Mapeamento do processo de gerenciamento de riscos de ativos de informação e de processamento	Todos os membros	Agosto/2019
			3.5 Mapeamento do processo de gerenciamento de acessos e uso de recursos de TIC	STIC	Agosto/2019
			3.6 Mapeamento do processo de gerenciamento e controle de ativos de informação e de processamento	STIC	Agosto/2019
			3.7 Mapeamento do processo de gerenciamento de incidentes de segurança da informação	STIC	Agosto/2019
			3.8 Mapeamento do processo de gerenciamento de continuidade de serviços essenciais de TIC	STIC	Agosto/2019
4	GESTÃO DE PESSOAS	CAPACITAR OS SERVIDORES DA COMISSÃO EM GESTÃO DA SEGURANÇA DA INFORMAÇÃO	4.1 Levantamento das necessidades de capacitação para 2020	Todos os membros	Agosto/2019 a Outubro/2019
			4.2 Execução das ações de capacitação da CPSI	SGP	1º semestre 2020
5		CAPACITAR USUÁRIOS DO TRE/RN EM SEGURANÇA DA INFORMAÇÃO	5.1 Elaboração de treinamento EAD em segurança da informação	STIC e SGP	Outubro a Novembro/2019
			5.2 Disponibilização de treinamento EAD em segurança da informação	SGP	1º semestre 2020
6	COMUNICAÇÃO INSTITUCIONAL	DISSEMINAR INFORMAÇÕES SOBRE SEGURANÇA DA INFORMAÇÃO, DE FORMA FÁCIL E ACESSÍVEL	6.1 Realizar o dia da segurança da informação	STIC e ASCOM	Março/2020
			6.2 Propor a criação de área de destaque para o tema "Segurança da Informação" na intranet do TRE, acessível a partir da página principal.	STIC	Agosto/2019
			6.3 Envio de informativos eletrônicos (mensal)	STIC e ASCOM	Contínuo
7	ALINHAMENTO ESTRATÉGICO	Indicador PEJERN IA-37 - Índice de gestão da segurança da informação (Garantir a evolução do sistema de gestão de segurança da informação, por meio da implantação dos controles previstos na norma ABNT ISO 27001/27002)	7.1 Ratificar a tabela-base de medição e responsáveis	Todos os membros	Setembro/2019
			7.2 Realizar medição do indicador	Todos os membros	Setembro/2019