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

ATA DE REUNIÃO N. 003/2019

I. Identificação da Reunião

Data	Horário		Local	Coordenador
	Início	Término		
25.11.19	13h30	14h00	Sala do Secretário de TIC	Marcos Flávio Nascimento Maia

II. Objetivo

Reunião da CPSI para tratar dos seguintes assuntos:

1. Atualização do Plano de Ação da CPSI;
2. Medição de 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	
Renato Vilar de Lima (suplente)	ASCOM/ PRES	
Rafael Fonseca Alves (suplente)	NSPRES/ PRES	
Ana Esmera Pimentel da Fonseca	AJCRE/CRE	
Fernanda Araújo Cruz Barbosa	GABDG	
Liliane Priscila Bezerra da Silva Miranda Gomes	CGI/SJ	
Zeneide Lobato Reis da Silva	~~SENG/CAP~~/SAOF	(GAPSAOF)
Fláuber Kley de Araújo Cândido	SRF/COPES/SGP	
Carlos André de Azevedo Moura (suplente)	COINF/STIC	
Daniel César Gurgel Coelho Ponte	SRI/COINF/ STIC	
Alexandre Márcio Cavalcanti Machado	SMI/COINF/ STIC	
Carlos Alberto Narciso Fernandes	SBDS/COSIS/ STIC	
Helder Jean Brito da Silva	SSI/COINF/STIC	

IV. Discussão da Pauta

Nº	Descrição/Decisão	Responsável
01	Plano de Ação da CPSI • O Plano de Ação validado na reunião de 09.08.2019 foi atualizado e proposto à Comissão. • O Plano foi aprovado pelos presentes, com os devidos ajustes propostos, conforme Anexo 1 desta Ata.	Marcos Maia
02	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) • A medição do indicador foi realizada pelo Presidente da Comissão e apresentada aos presentes. • A medição foi aprovada pelos presentes, conforme anexo 2 desta ata.	Marcos Maia

V. Pendências Identificadas

Nº	Pendências	Responsável	Data limite
01	Analisar meta adequada para 2020 para o indicador IA-37 do PEJERN e encaminhar proposta para a próxima RAE, prevista para janeiro/2020.	Marcos Maia	19.12.2019
02	Encaminhar ao Presidente da Comissão a necessidade de capacitação própria na área de segurança da informação, conforme ação 4.1 do Plano.	Todos os integrantes da CPSI	09.12.2019

V. Fechamento da Ata

Data	Nome do relator	Assinatura
25.11.19	Dina Márcia de V. Maranhão da Câmara	

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

ANEXO 1

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	Andamento
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	Publicação da Resolução n.º 20/2019 - PSI
			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	Res. TRE/RN n. 15/2016 Res. TRE/RN n. 22/2016
			2.2 Gestão de Riscos de Ativos de Informação e de Processamento	Todos os membros	~~Agosto/2019~~ 1º semestre 2020	
			2.3 Controle de Acessos e Usos de Recursos de TIC	Todos os membros	Agosto/2019	Atualmente, existem as portarias n. 99/2015 - GP (acesso à rede wi fi) e n. 45/2018-GP (acesso a sistemas)
			2.4 Gestão de Ativos de Informação e de Processamento	STIC	Agosto/2019	Portaria n. 195/2019-GP (modelagem do processo)
			2.5 Gestão de Incidentes de Segurança da Informação	STIC	Agosto/2019	Portaria n. 185/2019-GP (modelagem do processo)
			2.6 Plano de Continuidade de Serviços Essenciais de TIC	STIC	Agosto/2019	A Gestão da Continuidade de Serviços Essenciais de TIC foi instituída por meio da Portaria n.177/2019-GP
3		PROCESSOS DE SEGURANÇA DA INFORMAÇÃO	3.1 Aprovação do Catálogo de Processos de Segurança da Informação	STIC	~~Agosto/2019~~ Janeiro a Fev/2020	
			3.2 Mapeamento do processo de elaboração, acompanhamento e revisão da Política de Segurança da Informação	Todos os membros	Agosto/2019	Portaria n. 182/2019-GP
			3.3 Mapeamento do processo de classificação e tratamento da informação	CPAD	Agosto/2019	Portaria n. 184/2019-GP
			3.4 Mapeamento do processo de gerenciamento de riscos de ativos de informação e de processamento	Todos os membros	~~Agosto/2019~~ 1º semestre 2020	
			3.5 Mapeamento do processo de gerenciamento de acessos e uso de recursos de TIC	STIC	Agosto/2019	Portaria n. 189/2019-GP - Gerenciamento de Controle de Acesso Lógico
			3.6 Mapeamento do processo de gerenciamento e controle de ativos de informação e de processamento	STIC	Agosto/2019	Portaria n. 195/2019 - GP - Gerenciamento de Configuração e Ativos de TIC
			3.7 Mapeamento do processo de gerenciamento de incidentes de segurança da informação	~~STIC~~ Todos os membros	Agosto/2019	Portaria n. 185/2019-GP
			3.8 Mapeamento do processo de gerenciamento de continuidade de serviços essenciais de TIC	STIC	Agosto/2019	A Gestaõ da Continuidade de Serviços Essenciais de TIC foi instituída por meio da Portaria n.177/2019-GP
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~~ Novembro a Dezembro/2019	
			4.2 Execução das ações de capacitação da CPSI	SGP	~~1º semestre 2020~~ Ano de 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~~ Janeiro a Março/2020	
			5.2 Disponibilização de treinamento EAD em segurança da informação	SGP	~~1º semestre 2020~~ Abril a Junho/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~~ Novembro 2019	Link para a página da Internet
			6.3 Envio de informativos eletrônicos (mensal)	STIC e ASCOM	Contínuo - A partir de 2020	

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	Andamento
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~~	
			7.1. Realizar medição do indicador	Todos os membros	~~Setembro/2019~~ Novembro/2019	
			7.2 Identificar e realizar ações para atendimento de alguns controle da NBR 27.001, visando ao cumprimento da nova meta estabelecida para o ano de 2020.	Todos os membros	1º semestre 2020	

ANEXO 2

IA37 - Índice de gestão de segurança da informação

Indicador de Apoio: IA37 - Índice de gestão da segurança da informação					
Indicador Estratégico: IE18 - Índice de gestão da segurança da informação *			**Peso (%)**	ANE	AE
				100	
Objetivo Estratégico: 9. Aprimoramento da infraestrutura, da gestão e da governança de TIC					
Tipo	Excelência	**Polaridade**	Quanto maior melhor		
O que mede	O nível de maturidade em gestão da segurança da informação.				
Para que medir	Garantir a evolução do sistema de gestão de segurança da informação, por meio da implantação dos controles previstos na norma ABNT ISO 27001/27002.				
Quem mede	Comissão Permanente de Segurança da Informação				
Periodicidade	Anual				
Como medir	Fórmula: ΣNotaIC / TIC, onde: NotaIC - Somatório da pontuação obtida em cada item de controle da norma ABNT ISO 27001/27002 implantados no período-base sendo: 0% - Não adota 25% - Iniciou providências para adotar o item de controle 50% - Adota parcialmente 100% - Adota em grande parte ou adota integralmente; e TIC - Total de itens de controle da norma ABNT ISO 27001/27002, considerados os 114 itens constantes do Anexo A				
Onde medir	Nos relatórios elaborados pela Comissão Permanente de Segurança da Informação.				
Histórico (%)	**2011**	**2012**	**2013**	**2014**	**2015**
	NA	NA	NA	NA	NA
Meta Prevista (%)	**2016**	**2017**	**2018**	**2019**	**2020**
	10	20	30	40	50
Meta Realizada (%)					
Observações sobre os resultados					

ANEXO A – Indicador 37					
ID	**Categoria**	**Subcategoria**	**ID**	**Descrição**	**Grau de Atendimento (0%, 25%, 50%, 100%)**
1	5.Políticas de segurança da Informação	5.1 Orientação da direção para segurança da informação	5.1.1	Políticas para segurança da informação	100
2			5.1.2	Análise crítica das políticas para segurança da informação	0
3	6. Organização da segurança da informação	6.1 Organização interna	6.1.1	Responsabilidades e papéis pela segurança da informação	100
4			6.1.2	Segregação de funções	100
5			6.1.3	Contato com autoridades	0
6			6.1.4	Contato com grupos especiais	0
7			6.1.5	Segurança da informação no gerenciamento de projetos	0
8		6.2 Dispositivos móveis e trabalho remoto	6.2.1	Política para o uso de dispositivo móvel	100
9			6.2.2	Trabalho remoto	100
10		7.1 Antes da contratação	7.1.1	Seleção	0
11			7.1.2	Termos e condições de contratação	0
12			7.2.1	Responsabilidades da direção	0

ANEXO A – Indicador 37					
ID	**Categoria**	**Subcategoria**	**ID**	**Descrição**	**Grau de Atendimento (0%, 25%, 50%, 100%)**
13	7. Segurança em recursos humanos	7.2 Durante a contratação	7.2.2	Conscientização, educação e treinamento em segurança da informação	50
14			7.2.3	Processo disciplinar	100
15		7.3 Encerramento e mudança da contratação	7.3.1	Responsabilidades pelo encerramento ou mudança da contratação	0
16	8. Gestão de Ativos	8.1 Responsabilidade pelos ativos	8.1.1	Inventário dos ativos	100
17			8.1.2	Proprietário dos ativos	100
18			8.1.3	Uso aceitável dos ativos	100
19			8.1.4	Devolução de ativos	100
20			8.2.1	Classificação da informação	100

ANEXO A – Indicador 37					
ID	**Categoria**	**Subcategoria**	**ID**	**Descrição**	**Grau de Atendimento (0%, 25%, 50%, 100%)**
21		8.2 Classificação da informação	8.2.2	Rótulos e tratamento da informação	100
22			8.2.3	Tratamento dos ativos	50
23		8.3 Tratamento das mídias	8.3.1	Gerenciamento de mídias removíveis	0
24			8.3.2	Descarte de mídias	0
25			8.3.3	Transferência física de mídias	0

ANEXO A – Indicador 37					
ID	**Categoria**	**Subcategoria**	**ID**	**Descrição**	**Grau de Atendimento (0%, 25%, 50%, 100%)**
26	9. Controle de acesso **(STIC)**	9.1 Requisitos do negócio para controle de acesso	9.1.1	Política de controle de acesso	100
27			9.1.2	Acesso às redes e aos serviços de rede	100
28		9.2 Gerenciamento de acesso ao usuário	9.2.1	Registro e cancelamento de usuário	100
29			9.2.2	Provisionamento para acesso de usuário	100
30			9.2.3	Gerenciamento de direitos de acesso privilegiados	100
31			9.2.4	Gerenciamento da informação de autenticação secreta de usuários	50
32			9.2.5	Análise crítica dos direitos de acesso de usuário	50
33			9.2.6	Retirada ou ajuste de direitos de acesso	100
34		9.3 Responsabilidades dos usuários	9.3.1	Uso da informação de autenticação secreta	50
35		9.4 Controle de acesso ao sistema e à aplicação	9.4.1	Restrição de acesso à informação	100
36			9.4.2	Procedimentos seguros de entrada no sistema (log-on)	50
37			9.4.3	Sistema de gerenciamento de senha	0
38			9.4.4	Uso de programas utilitários privilegiados	100
39			9.4.5	Controle de acesso ao código-fonte de programas	0
40	10. Criptografia	10.1 Controles criptográficos	10.1.1	Política para o uso de controles criptográficos	0
41			10.1.2	Gerenciamento de chaves	0
42			11.1.1	Perímetro de segurança física	50
43			11.1.2	Controles de entrada física	100
44			11.1.3	Segurança em escritórios, salas e instalações	100

ANEXO A – Indicador 37					
ID	**Categoria**	**Subcategoria**	**ID**	**Descrição**	**Grau de Atendimento (0%, 25%, 50%, 100%)**
45	11. Segurança física e do ambiente	11.1 Áreas seguras	11.1.4	Proteção contra ameaças externas e do meio-ambiente	50
46			11.1.5	Trabalhando em áreas seguras	100
47			11.1.6	Áreas de entrega e de carregamento	100
48		11.2 Equipamento	11.2.1	Localização e proteção do equipamento	50
49			11.2.2	Utilidades	100
50			11.2.3	Segurança do cabeamento	100
51			11.2.4	Manutenção dos equipamentos	100
52			11.2.5	Remoção de ativos	100
53			11.2.6	Segurança de equipamentos e ativos fora das dependências da organização	100
54			11.2.7	Reutilização e alienação segura de equipamentos	0
55			11.2.8	Equipamento de usuário sem monitoração	50
56			11.2.9	Política de mesa limpa e tela limpa	50

ANEXO A – Indicador 37					
ID	**Categoria**	**Subcategoria**	**ID**	**Descrição**	**Grau de Atendimento (0%, 25%, 50%, 100%)**
57	12. Segurança nas operações	12.1 Responsabilidades e procedimentos operacionais	12.1.1	Documentação dos procedimentos de operação	100
58			12.1.2	Gestão de mudanças	25
59			12.1.3	Gestão de capacidade	50
60			12.1.4	Separação dos ambientes de desenvolvimento, teste e de produção	100
61		12.2 Proteção contra malware	12.2.1	Controles contra códigos maliciosos	100
62		12.3 Cópias de segurança	12.3.1	Cópias de segurança das informações	100
63		12.4 Registro e monitoramento	12.4.1	Registros de eventos	50
64			12.4.2	Proteção das informações dos registros de eventos (logs)	100
65			12.4.3	Registros de eventos (log) de administrador e operador	100
66			12.4.4	Sincronização dos relógios	100
67		12.5 Controle de software operacional	12.5.1	Instalação de software nos sistemas operacionais	100
68		12.6 Gestão de vulnerabilidades técnicas	12.6.1	Gestão de vulnerabilidades técnicas	50
69			12.6.2	Restrições quanto à instalação de software	100
70		12.7 Considerações quanto à auditoria de sistemas da informação	12.7.1	Controles de auditoria de sistemas de informação	0
71	13. Segurança nas comunicações	13.1 Gerenciamento da segurança em redes	13.1.1	Controles de redes	100
72			13.1.2	Segurança dos serviços de rede	100
73			13.1.3	Segregação de redes	100
74		13.2 Transferência de informação	13.2.1	Políticas e procedimentos para transferência de informações	50
75			13.2.2	Acordos para transferência de informações	0
76			13.2.3	Mensagens eletrônicas	100
77			13.2.4	Acordos de confidencialidade e não divulgação	0
78		14.1 Requisitos de segurança de sistemas de informação	14.1.1	Análise e especificação dos requisitos de segurança da informação	0
79			14.1.2	Serviços de aplicação seguros em redes públicas	0
80			14.1.3	Protegendo as transações nos aplicativos de serviços	0
81			14.2.1	Política de desenvolvimento seguro	0

ANEXO A – Indicador 37					
ID	**Categoria**	**Subcategoria**	**ID**	**Descrição**	**Grau de Atendimento (0%, 25%, 50%, 100%)**
82	14. Aquisição, desenvolvimento e manutenção de sistemas	14.2 Segurança em processos de desenvolvimento e de suporte	14.2.2	Procedimentos para controle de mudanças de sistemas	25
83			14.2.3	Análise crítica técnica das aplicações após mudanças nas plataformas operacionais	25
84			14.2.4	Restrições sobre mudanças em pacotes de Software	50
85			14.2.5	Princípios para projetar sistemas seguros	0
86			14.2.6	Ambiente seguro para desenvolvimento	100
87			14.2.7	Desenvolvimento terceirizado	100
88			14.2.8	Teste de segurança do sistema	25
89			14.2.9	Teste de aceitação de sistemas	25
90		14.3 Dados para teste	14.3.1	Proteção dos dados para teste	25
91	15. Relacionamento na cadeia de suprimento	15.1 Segurança da informação na cadeia de suprimento	15.1.1	Política de segurança da informação no relacionamento com os fornecedores	0
92			15.1.2	Identificando segurança da informação nos acordos com fornecedores	0
93			15.1.3	Cadeia de suprimento na tecnologia da comunicação e informação	0
94		15.2 Gerenciamento da entrega do serviço do fornecedor	15.2.1	Monitoramento e análise crítica de serviços com fornecedores	0
95			15.2.2	Gerenciamento de mudanças para serviços com fornecedores	0
96	16. Gestão de incidentes de segurança da informação	16.1 Gestão de incidentes de segurança da informação e melhorias	16.1.1	Responsabilidades e procedimentos	50
97			16.1.2	Notificação de eventos de segurança da informação	50
98			16.1.3	Notificando fragilidades de segurança da informação	50

ANEXO A – Indicador 37					
ID	**Categoria**	**Subcategoria**	**ID**	**Descrição**	**Grau de Atendimento (0%, 25%, 50%, 100%)**
99			16.1.4	Avaliação e decisão dos eventos de segurança da informação	50
100			16.1.5	Resposta aos incidentes de segurança da informação	50
101			16.1.6	Aprendendo com os incidentes de segurança da informação	50
102			16.1.7	Coleta de evidências	0
103	17. Aspectos da segurança da informação na gestão da continuidade do negócio	17.1 Continuidade da segurança da informação	17.1.1	Planejando a continuidade da segurança da informação	0
104			17.1.2	Implementando a continuidade da segurança da informação	0
105			17.1.3	Verificação, análise crítica e avaliação da continuidade da segurança da informação	0
106		17.2 Redundâncias	17.2.1	Disponibilidade dos recursos de processamento da informação	100
107	18. Conformidade	18.1 Conformidade com requisitos legais e contratuais	18.1.1	Identificação da legislação aplicável e de requisitos contratuais	0
108			18.1.2	Direitos de propriedade intelectual	100
109			18.1.3	Proteção de registros	25
110			18.1.4	Proteção e privacidade de informações de identificação pessoal	0
111			18.1.5	Regulamentação de controles de criptografia	0
112		18.2 Análise crítica da segurança da informação	18.2.1	Análise crítica independente da segurança da informação	0
113			18.2.2	Conformidade com as políticas e procedimentos de segurança da informação	25
114			18.2.3	Análise crítica da conformidade técnica	25
				Soma das notas obtidas em cada item de controle formalmente implantados no TRE-RN	**5925**
				Total de itens de controle	**114**
				Porcentagem de atendimento	**51,97**