

ATA DE REUNIÃO CONJUNTA CDTIC E CSI**Código de Classificação: 011**

ORIGEM:	COMITÊ DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (CDTIC) COMISSÃO DE SEGURANÇA DA INFORMAÇÃO (CSI)
LOCAL:	Remoto – via MS Teams
DATA:	29/07/2021 14h

Fase corrente: 4 anos
Fase intermediária: 5 anos
Destinação Final: Guarda permanente

Participantes

Unidade	Representantes
Diretoria Geral	Hugo Pereira Filho
Secretaria de Tecnologia da Informação (STI) – Presidente do CDTIC	Lorena de Almeida Morais Belo
Secretaria de Administração (SAD)	Benedito Sérgio Monte Silva Coelho
Secretaria da Corregedoria Regional Eleitoral (SCR)	Maria Cecília de Sá Arruda
Secretaria de Gestão de Pessoas (SGP)	Cyntia Monteiro Dantas Toscano
Secretaria de Orçamento e Finanças (SOF)	Iberê Comin Nunes
Secretaria Judiciária (SJU)	Orleanes Cavalcanti de Oliveira Viana Gomes
Assessoria de Planejamento e Gestão da Diretoria-Geral (ASPEG)	José Romaico de Carvalho
Coordenadoria de Infraestrutura Tecnológica (COINT)	Jonas de Araújo Luz Junior
Coordenadoria de Sistemas (COSIS)	Laerton Misael Vasques Ferreira
Núcleo de Governança e Gestão de Tecnologia da Informação e Comunicação (NGT)	Alexandre Monteiro Paulo
Seção de Suporte Operacional e Segurança da Informação (SESI)	Sandra Cassiano Rodrigues

Pauta e deliberações

Item	Pauta / Proposta / Questão / Deliberação	Autores	Responsáveis	Prazo
1	Apresentação - Plano Diretor de Tecnologia da Informação (PDTI) 2021-2026			
	1. O PDTI relativo aos membros do CDTIC. 2. Após elogiar o trabalho realizado pela STI e NGT, a ASPEG apresentou sugestões ao texto: 2.1. A referência ao PETI da JE deve ser retirada, já que a referida norma nunca foi publicada. 2.2. O Anexo I (Matriz de Riscos) não segue estritamente a metodologia e modelos adotados pelo TRE/CE para matrizes de risco. Sugere-se que o referido anexo seja considerado e intitulado como um levantamento geral de riscos identificados. 2.3. Sugere-se que a oportunidade do PDTI seja utilizada para melhorar os indicadores que não obtiveram pontuação no último levantamento de governança do TCU, a saber:	STI e NGT	STI e NGT	-

	<p>a) Política de controle de acesso; b) Métricas de qualidade de software; c) Plano de dados abertos.</p> <p>3. Considerações às sugestões da ASPEG: 3.1. Em resposta ao item 2.3.a representante da SESIS esclareceu que, estando a questão da política de acesso inserida no contexto da norma ABNT ISO/IEC 27001, já se encontra contemplada pelo PDTI. 3.2. Com relação ao Plano de Dados Abertos, o representante da COSIS destacou que este deve ser trabalhado em sintonia com a implementação da LGPD, sob pena de haver conflito entre estes. Deste modo, caso o Plano de Dados Abertos venha a ser contemplado no âmbito do Plano de Tratamento de Dados (PTD), e como este último há de ser coordenado pelo TSE, a ingerência do TRE/CE sobre isto será limitada.</p> <p>4. O PDTI foi aprovado contemplando-se as sugestões apresentadas pela ASPEG com as ressalvas feitas pela STI e SESIS.</p>			
2	Priorização das demandas de desenvolvimento de software.			
	<p>5. STI e COSIS apresentaram nova demanda para consideração do CDTIC: 5.1. PAD 017461/2020 Demandante: SEAPE. Objeto: sistema de contagem do tempo de contribuição dos servidores ativos.</p> <p>6. A demanda apresentada foi aprovada pelo comitê para entrar no rol de demandas.</p> <p>7. O representante da COSIS relatou que as equipes da COSIS atendem não somente às demandas internas, mas também às demandas dos órgãos de controle externo. 7.1. A representante da SJU pontuou a necessidade de formação de equipe específica para atender as demandas dos órgãos de controle externo.</p> <p>8. Por fim, o representante da COSIS também solicitou às áreas demandantes que reavaliassem seus pedidos mantidos em histórico, de forma a retirar aqueles que, por qualquer razão, tenham perdido o objeto ou possam ser sanados de outra forma.</p>	STI / COSIS	STI / COSIS	-
3	PAD n.º 10512/2021 - Acesso à rede do TRE pelo servidor em teletrabalho no exterior			
	<p>9. Dos riscos. A representante da SESIS informou dos riscos de se abrir o acesso à VPN a partir do exterior. Elencau que há três servidores nesta situação, sendo que o caso apresentado no processo em tela resta pendente de liberação por não conseguir obter IP fixo ou serviço de "máscara".</p> <p>10. Do alto custo de contratação de IP fixo pelo usuário. O representante da COINT esclareceu que serviços de IP fixo são, geralmente, contratados por empresas, sendo mais onerosos e se justificam, por exemplo, quando se quer prover algum serviço na internet, como é o caso do TRE/CE. Explicou que, deste modo, não é comum a contratação de IPs fixos por pessoas físicas que desejem apenas o acesso à rede mundial de computadores.</p> <p>11. Adicionalmente, o coordenador da COINT, durante a reu-</p>	COINT e SESIS	COINT e SESIS	

<p>ção, confirmou, por mensagem, com dois usuários – Rafael Paz e Raquel Gadelha – que estes não fizeram nenhuma contratação diferenciada quando de sua estada no exterior e, após liberação de seus IPs pela SESIC, o acesso se deu normalmente.</p> <p>12. Os representantes da COINT e da SESIC apresentaram as alternativas de solução para o caso:</p> <p>a) Liberação do IP do usuário, conforme informado por ele, que deverá renovar a solicitação a cada mudança de seu IP de acesso. Esta é a opção de menor risco.</p> <p>b) Liberação de uma subfaixa dos IPs da sub-rede da operadora do usuário, a fim de reduzir a necessidade de renovação do pedido de liberação. Esta opção traz maior risco à operação.</p> <p>12.2. Adicionalmente, o representante da COINT enfatizou a necessidade de que o usuário comunique também seu retorno do exterior, de forma que a liberação do IP estrangeiro possa ser desabilitada.</p> <p>12.3. Após deliberação do CSI, ficou resolvido que a primeira opção será adotada, incluindo a comunicação de retorno do exterior, conforme item anterior.</p>			
4 Proposta de duplo fator de autenticação para acesso à rede do TRE via VPN Web			
<p>13. Dos riscos. Os representantes da COINT e SESIC apresentaram os riscos existentes do acesso à VPN web (SSL) apenas por meio de credenciais usuário/senha.</p> <p>14. Da solução proposta. Na sequência, os representantes da COINT e SESIC explicaram a necessidade de se fazer uso do duplo fator de autenticação (<i>2-factor authentication</i> ou 2FA). Explicaram também que, no cenário atual, apenas é viável, a curto prazo, a implementação do 2FA com envio do código de acesso ao endereço de e-mail pessoal de cada usuário, o que exige que estes endereços estejam atualizados no cadastro de pessoal.</p> <p>14.1. A SGP lembrou que a atualização dos dados pessoais já foi solicitada e deve ser feita por todos os usuários.</p> <p>15. O representante da COINT, adicionalmente, conclamou que todos tomem parte na garantia da segurança da informação do TRE/CE, o que não é uma responsabilidade somente da COINT ou da SESIC. Especificamente, solicitou que se evitasse o uso de senhas fracas, como 12345678 ou as iniciais do próprio nome.</p> <p>16. A proposta de implementação foi aprovada pela CSI.</p>	COINT e SE SIC	COINT e SE SIC	

Aprovações

Os representantes das unidades presentes a esta reunião aprovam as deliberações desta ata, e, para tanto, a assinam eletrônica ou digitalmente.

Fortaleza, CE, datas registradas nas assinaturas.