ATA - TRE-AP/PRES/DG/STI

COMISSÃO DE SEGURANÇA DA INFORMAÇÃO

Portaria Nº 43/2021 (ID SEI 0513623)

Ata de Reunião

1. Dados da Reunião

Data: 09/09/2021	**Início:** 15h	**Término:** 16h10	**Local:** Videoconferência – Ferramenta Zoom
Pauta	1. Adoção de Controles de Segurança 2. Alinhamento de Normas de Segurança da Informação do TRE-AP ao CNJ e TSE		

2. Participantes

Nome	Cargo	Função
Emanoel dos Santos Flexa	Secretário da STI	Presidente
Maria Eliane de Souza Oliveira	Secretária da SGP	Membro
Dilma Célia de Oliveira Pimenta	Secretária da SAO	Membro
Mylene Lages Mendes de Azevedo	Secretária da SEJUD	Membro
Jimmy Almendra Macedo	Coordenador da CINF	Membro
Adeilson Mendes	Assessor da ASDG	Membro (ausente por estar em férias)

3. Assuntos Tratados e Deliberações

O servidor **Emanoel Flexa** iniciou a reunião informando que o objetivo principal da reunião é deliberar sobre controles de segurança a serem implementados nos sis expostos na Internet. Citou também que apresentaria deliberação inicial sobre novas normas a serem criadas no Tribunal sobre Segurança da Informação.

Item 1. Adoção de Controles de Segurança

O Presidente da Comissão destacou, inicialmente, que o TSE apresentou recentemente às STI's dos Tribunais Regionais a Estratégia Nacional de Seguran Informação da Justiça Eleitoral, a qual será apresentada a todos os Presidentes dos Tribunais Regionais Eleitorais no dia 10/09/2021, em evento do COPTREL ded para o tema, a qual, entre as proposições apresentadas, destaca a necessidade de haver unidade e servidores dedicados exclusivamente à Cibersegurança dentro de STI dos regionais. Além disso, citou também que a estratégia prevê a criação de estrutura ligada diretamente à alta administração, desvinculada da STI, para tra Gestão de Segurança da Informação. Citou que a estratégia é ampla e aborda os eixos de pessoas e unidades, políticas, ferramentas, serviços e sensibiliza conscientização.

Em seguida, informou que as propostas a serem apresentadas visam fortalecer a Segurança da Informação do Tribunal e reduzir os riscos de incidentes e at cibernéticos contra o Tribunal, considerando boas práticas de segurança da informação, como: autenticação em múltiplos fatores, controle de acessos, reduç superfície de ataque e não utilização de aplicações desatualizadas.

Foram apresentadas propostas onde a disponibilidade dos sistemas dar-se-á em dias e horários determinados, devido aos seguintes motivos:

1. Não há regulamentação de regime de plantão ou sobreaviso no tribunal para os servidores da STI. Desta forma, não há monitoramento ativo de pessoal das aplic disponibilizadas na Internet e nem respostas às tentativas de ataque e invasão à rede do Tribunal durante os finais de semana ou, nos dias de semana, entre 21h e da manhã.
2. Carência de pessoal na STI do TRE-AP, conforme detalhado no Relatório (ID SEI 0530908), que faz estudo da força de trabalho ideal da Secretaria de Tecnolog Informação (STI) do Tribunal Regional Eleitoral do Amapá (TRE-AP), conforme estabelecido no Guia CNJ da Estratégia Digital do Poder Judiciário 2021-202 referente à Resolução CNJ 370/2021.
3. Falta de estrutura organizacional adequada na STI/TRE-AP, conforme Relatório (ID SEI 0530927), criado com objetivo de apresentar proposta de estrutura organizacional ideal para a STI e que sugere a criação de mais uma coordenadoria e **dobrar o número de seções existentes na unidade**; entre elas, uma seção dedicada e específica para Cibersegurança.
4. Ainda não há ferramentas avançadas de monitoramento da rede visando que visam reduzir os riscos identificados
5. Falta de implementação de duplo fator de autenticação (2FA) nas aplicações nos itens 2 a 4 da Tabela 1

Para todas as aplicações expostas na internet e que fazem acesso à rede local, em especial aquelas que usam autenticação e ainda não usam 2FA (itens 2 a 4), o Presi da Comissão enfatizou da necessidade de utilização desse mecanismo de autenticação, bem como ampliação de estrutura de monitoramento automatizado e utilizaç ferramentas tecnológicas de alto desempenho para Segurança da Informação, tais como como Firewall de Borda (que funciona como um filtro, verifi constantemente o fluxo de dados na organização, analisando sua procedência), Softwares de Gestão de Vulnerabilidades, SIEM (ferramentas que apresentam relató alertas) dentre outros. Acrescentou ainda que precisa de equipes dedicadas dentro da STI para realização e adoção destes controles.

Em seguida, ressaltou que, considerando que a STI ainda não possui servidores com dedicação exclusiva para cibersegurança e que ainda não possui os recu ferramentas tecnológicas mencionados, a melhor solução a ser adotada seria realizar o bloqueio de acesso das aplicações externas que fazem acesso aos recursos de locais do TRE-AP. Porém, a comissão entendeu que o bloqueio total, para algumas aplicações, teria profundo impactos nos serviços prestados, em especial para ac servidores em trabalho remoto ou para público externo na utilização de alguns recursos, tais como a consulta de ata e pautas de sessões.

Para facilitar a discussão e deliberação dos itens a serem abordados, foi apresentada a "Tabela 1. Sistemas de TI disponibilizados na Internet", a qual contém, entre informações, a lista atual de sistemas expostos na Internet, a situação atual desses sistemas e as propostas de controles a serem implementados.

Baseado nas ponderações gerais apresentadas e nas deliberações realizadas para cada sistema, a tabela foi atualizada e aprovada pela comissão, conforme aprese abaixo.

Solicitou atenção às colunas "Situação Atual", que representa a disponibilidade atual do sistema na Internet, e a coluna "Proposta", que representa proposiç disponibilidade do sistema e reforçou que os controles apresentados são dinâmicos e que é natural outras revisões futuras desses controles, que podem ser ser alte para mais ou menos restritos, conforme acréscimo de mais servidores e unidades na STI, os quais poderão ser utilizados para dedicação exclusiva à Cibersegu aquisições de novas ferramentas específicas de Segurança e de eventuais novas interpretações das propostas e riscos apresentados.

Item	Recurso	Setor Gestor do Sistema	Tipo de Usuário e Acesso	Situação Atual	Proposta Novo dia/horário de funcionamento	Ações adicionais planejadas (além da proposta)	Pode solicitar exceção à regra?	Quem autoriza	Link de acesso
1	VPN	STI	Interno (Com Autenticação)	Liberado Todos os Dias - 24h	Segunda a Sexta 7h - 21h *Para o serviço de e-mail, além a proposição de horário de funcionamento, bloquear redirecionamento de e-mails do TRE-AP para e-mails externos.*	1. Restringir acesso na rede local. 2. Revisão de acessos dos usuários.	Sim	DG	NetExtender
2	Sistema SEI (acesso externo)					1. Atualizar sistema SEI para sua última versão, a qual possui o recurso de 2FA. O STI informou que a ação depende da liberação do TRF-4, o qual já foi oficiado, porém ainda não deu resposta ao TRE-AP.	Não	N/A	https://sei.tre-ap.jus.br/sei/
3	Email Corporativo (acesso externo)					1. Migrar para serviço de e-mail em nuvem adquirido pelo TRE-AP (Outlook) com 2FA. 2. Restringir redirecionamento de e-mail	Não	N/A	https://sistemas.tre-ap.jus.br/webmail/
4	Cloud TRE-AP (Acesso externo)				Bloquear temporariamente, ate efetivo início do contrato em nuvem do TRE.	1. Migrar para serviço de e-mail em nuvem adquirido pelo TRE-AP (OneDrive) com 2FA.	Não	N/A	https://sistemas.tre-ap.jus.br/cloud/
5	Consulta de Diárias	SGP	Externo (Sem Autenticação)	Liberado Todos os Dias - 24h	Bloquear.	1. Usar portal da transparência do CNJ.	Não	N/A	https://sistemas.tre-ap.jus.br/diarias-portal-transparencia
6	Transparência Servidores				Segunda a Sexta 7h - 21h	1. Tentar solução mais recente com o TSE 2. Revisar Infraestrutura da aplicação.	Não	N/A	https://apps.tre-ap.jus.br/transparenciaDadosServidores/
7	Consulta de Pauta de Sessões	SEJUD	Externo (Sem Autenticação)	Liberado Todos os Dias - 24h	Todos os dias 7h - 21h	1. Utilizar Portal de Internet do TRE-AP para realizar publicação de pautas, atas e calendários das sessões. 2. STI estudar, caso necessário, solução adicional para utilização no futuro.	Não	N/A	https://www.tre-ap.jus.br/servicosjudiciais/sessao-plenaria/calendario-de-sessoes-plenarias
8	Consulta SGIP				Bloquear Internet	1. Retirar da Internet e deixar somente para consulta interna	Não	N/A	http://10.25.1.182:8600/consulta-sgip
9	Consulta Licitações (antigas - 2019)	SAO	Externo (Sem Autenticação)	Liberado Todos os Dias - 24h	Bloquear Internet	1. STI deve buscar solução de contorno para publicar as licitações anteriores à 2019.	Sim	CGTIC	https://www.tre-ap.jus.br/transparencia-e-prestacao-de-contas/licitacoes/lista-de-licitacoes
10	Consulta Licitações (recentes)				Segunda a Sexta 7h - 21h	1. Revisar Infraestrutura da aplicação.	Sim	CGTIC	https://sei.tre-ap.jus.br/licitacoes/index.php?tipo=PREGAO_ELETRONICO
11	Módulo Ouvidoria	OUVI	Externo (Sem Autenticação)	Liberado Todos os Dias - 24h	Segunda a Sexta 7h - 21h	1. Revisar Infraestrutura da aplicação.	Sim	CGTIC	
12	Moodle	CEJE	Externo e Interno (Com Autenticação)	Liberado Todos os Dias - 24h	Liberado Todos os Dias - 24h	1) Adotar 2FA para Administradores 2) Autenticação p/ público externo (google, MS, Facebook)	N/A	N/A	https://https://eadeje.tse.jus.br/
13	Eleitor do Futuro			Liberado Todos os Dias - 24h	Segunda a Sexta 7h - 21h	1) Adotar 2FA para Administradores	Não	N/A	https://eleitordofuturo.tre-ap.jus.br/
14	Sistema PJE	SEJUD	Gestão do TSE. Sem necessidade de deliberação.						https://www.tre-ap.jus.br/servicos-judiciais/processo-judicial-eletronico-pje
15	Sistema de Petição Eletrônica	SEJUD							https://inter03.tse.jus.br/peticao/do/autenticar
16	Sistema SIEL (qualquer acesso)	CRE							https://www.tre-ap.jus.br/servicos-judiciais/sistemas-de-informacoes-eleitorais-siel
17	Infodip (Acesso externo)	CRE							https://apps.tre-ap.jus.br/infodipweb

Tabela 1. Sistemas de TI disponibilizados na Internet

Em relação ao item 4 da tabela, além da proposta de horário e dia de funcionamento, o Presidente da Comissão fez a proposição de proibir todo e qua redirecionamento de e-mail interno do TRE-AP para e-mails externos, apresentando as seguintes justificativas.

1. Alguns usuários utilizam o recurso de redirecionamento dos seus e-mails institucionais para suas contas externas (Gmail, Yahoo, Hotmail, etc) ou contas institu vinculados ao órgão de origem.
2. A STI não possui e não deve possuir nenhum tipo de controle sobre as contas externas pessoais ou institucionais utilizadas nos redirecionamentos. Em caso de eventual incidente de Segurança da Informação, o TRE-AP não poderá acessar essas contas para a realizar a investigação do incidente.
3. Nas contas externas, as senhas, configurações de compartilhamentos e ajustes gerais de segurança utilizados pelos usuários podem possuir controles menos restr que os controles atualmente adotados neste Tribunal, gerando
4. Os fatores acima elencados, que não são exaustivos, **aumentam os riscos de vazamento de dados institucionais e a superfície de ataques relacionados à e-m** consequentemente, à nossa rede corporativa.
5. O servidor de e-mail do TRE-AP **está disponível para acesso externo** para qualquer usuário com computador conectado à Internet

Após apresentação destes pontos, o bloqueio de redirecionamento de e-mail internos para e-mails externos também foi aprovado pela comissão.

Item 2. Alinhamento de Normas de Segurança da Informação do TRE-AP ao CNJ e TSE

O STI informou que iniciou trabalho de revisão da Política de Segurança da Informação do TRE-AP, a qual será baseada na Política de Segurança da Informaç Justiça Eleitoral (PSI-JE), recentemente publicada pelo TSE.

Comunicou que a PSI-JE, embora alinhada à Resolução CNJ 396-2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-P. alguns possui divergências de nomenclaturas ou funções, como, por exemplo:

- A PSI-JE cita Comissão de Segurança da Informação, enquanto a ENSEC-PJ cita Comitê Gestor de Segurança da Informação.
- O Comitê Gestor de Segurança da Informação da ENSEC-PJ possui responsabilidade mais direta sobre o Sistema de Gestão de Segurança da Informação que a Comissão de Segurança da Informação proposta na PSI-JE
- A ENSEC-PJ determina, em seu artigo 21º, que cada Tribunal, com exceção do STF, deve constituir estrutura de segurança da informação, subordinada diretam alta administração do órgão e desvinculada da área de TIC; enquanto a PSI-JE não deixa essa desvinculação com a STI

Após os exemplos acima, a comissão decidiu que, inicialmente, caso não haja divergência clara, deve-se seguir as recomendações do CNJ.

Por fim, agradeceu a presença e participação de todos e reforçou a necessidade de fortalecimento da Segurança da Informação, com as ponderações apresentad reunião, e com adoção das medidas a serem propostas na Estratégia Nacional de Cibersegurança do TSE.

Documento assinado eletronicamente por **DILMA CELIA DE OLIVEIRA PIMENTA**, **Secretário(a)**, em 11/09/2021, às 08:11, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **EMANOEL DOS SANTOS FLEXA**, **Secretário(a)**, em 14/09/2021, às 11:20, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MARIA ELIANE DE SOUZA OLIVEIRA**, **Secretário(a)**, em 14/09/2021, às 14:06, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **JIMMY ALMENDRA MACEDO**, **Coordenador(a)**, em 15/09/2021, às 14:34, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MYLENE LAGES MENDES AZEVEDO**, **Secretário(a)**, em 22/09/2021, às 14:37, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-ap.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0548505** e o código CRC **7AD78CF5**.