TRIBUNAL REGIONAL ELEITORAL DO AMAPÁ

COMITÊ DE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

Portaria nº 32/2023 **(SEI 0698904)**

1. DADOS DA REUNIÃO:

Data: 05/01/2026	**Início:** 16h	**Término:** 17h10	**Local:** Sala de reuniões da DG
Pauta	• Revisão da Política de Segurança da Informação • Mitigação de Riscos de Segurança da Informação - Acessos Internacionais • Gerenciamento do Plano do Gestão de Riscos • Ações de Conscientização e Treinamento Segurança • Bloqueio de acesso a dispositivos pessoais e removíveis de armazenamento de dados (Ofício-Circular CNJ nº 313/2025/SG)		

2. PARTICIPANTES:

Nome	Cargo	Função
Emanoel dos Santos Flexa	Secretário de Tecnologia da Informação	Presidente
Dilma Célia de Oliveira Pimenta	Diretoria-Geral	Convidada
Elinete Nunes Freitas	Secretária de Administração e Orçamento	Membra
Mylene Lages Mendes	Secretária Judiciária	Membra
Heverton Luiz Rodrigues Fernandes	Secretário de Gestão de Pessoas	Membro
Breno Borges Vasconcelos	Coordenador da Corregedoria	Membro
Adeilson Batista Mendes	Assessor Jurídico da Diretoria-Geral	Membro

3. ASSUNTOS TRATADOS E DELIBERAÇÕES:

O Secretário de Tecnologia da Informação e Gestor de Segurança da Informação, Emanoel Flexa, iniciou a reunião agradecendo a presença de todos e da Diretora-Geral, convidada da reunião, e agradecendo a compreensão com os empecilhos de adiamento e confirmação da reunião solicitados pelo gabinete.

Item 1 – Revisão da Política de Segurança da Informação

Apresentação:

O Gestor de Segurança da Informação, Emanoel Flexa, informou que o TSE apresentou minuta de uma nova política de segurança da informação (PSI) para a Justiça Eleitoral (JE). Informou também que na época da criação da atual PSI da JE, o TRE-AP havia decido por criar sua própria PSI, alinhada à PSI do TSE.

Recentemente o TSE apresentou minuta da nova PSI que será proposta para a JE. Desta forma, o TRE-AP deve novamente deliberar sobre o tema, assim como atualizar a PSI atual.

Neste sentido, o Gestor de Segurança da Informação opinou sobre manter a PSI do TRE-AP, atualmente disponível pela Resolução 616/2025, mas atualizá-la com alguns aspectos da minuta proposta do TSE, com destaque para realização de correções materiais, para inclusão de referência à Lei Geral de Proteção de Dados (LGPD), inclusão da obrigatoriedade de normas táticas para teletrabralho, computação em nuvem e inteligência artificial, assim como inclusão menção para Estratégia de Cibersegurança e Maturidade.

Após discussões gerais, ficou decidido pelos seguintes aspectos:

Deliberações:

- TRE-AP deve manter Política de Segurança da Informação própria.
- CGSI deve deliberar novamente sobre a PSI do TRE-AP após publicação efetiva da nova PSI do TSE.
- O Gestor de Segurança da Informação deve ajustar minuta para:
  - Incluir referências à LGPD
  - Incluir normas de Nível Tático (art. 9º, Inciso II) para Teletrabralho, Nuvem e IA.
  - Incluir aspectos relacionados à Estratégia de Cibersegurança e Maturidade
- A STI, por meio do Gestor de Segurança da Informação deve consolidar as propostas e encaminhar para publicação.

Item 2 – Mitigação de Riscos de Segurança da Informação - Acessos Internacionais

Apresentação:

O Secretário de Tecnologia da Informação e Gestor de Segurança da Informação apresentou proposta de bloqueio de acessos internacionais aos serviços de e-mail institucional, VPN e de acesso ao SEI, como medida técnica de mitigação de riscos com foco na redução da superfície de ataque à rede do TRE-AP.

Esclareceu que esses serviços concentram dados sensíveis e credenciais privilegiadas e são, historicamente, vetores preferenciais para ataques de força bruta, *credential stuffing, phishing* direcionado, exploração de vulnerabilidades conhecidas e tentativas de comprometimento de contas, grande parte delas originadas fora do território nacional. O STI informou que a proposta de bloqueio geográfico atua diretamente na redução da probabilidade de ocorrência desses eventos de risco, sem depender exclusivamente de controles reativos.

Ressaltou que e trata de um controle preventivo, de baixo impacto operacional e alta efetividade, amplamente recomendado em ambientes que tratam informações institucionais e dados pessoais. Destacou, ainda, que a proposta não inviabiliza acessos legítimos em situações excepcionais, uma vez que poderão ser concedidas liberações pontuais e temporárias, mediante análise de risco e aplicação de controles adicionais, preservando o equilíbrio entre segurança, disponibilidade e continuidade do serviço.

Por fim, registou que a adoção do bloqueio contribui para o atendimento às diretrizes de gestão de riscos, segurança da informação e proteção de dados, reduzindo a exposição a incidentes e fortalecendo a postura de segurança do TRE-AP de forma proporcional e tecnicamente justificada, tendo em vista que poucas vezes há pedidos de acessos de usuários no exterior, e não há pessoas em teletrabalho morando no exterior.

Deliberações:

- STI deve bloquear acessos internacionais
- STI de liberar acessos internacionais somente em caso de teletrabalho, caso haja viabilidade técnica, ou em casos excepcionais, havendo viabilidade técnica e autorizado pela diretoria-geral.

Item 3 – Gerenciamento do Plano do Gestão de Riscos

Apresentação:

No item relativo à gestão de riscos, foi apresentada e discutida a necessidade de atualização do Plano de Gestão de Riscos, em razão do avanço do uso de computação em nuvem no âmbito institucional e dos riscos associados a esse modelo tecnológico.

Destacou a importância de incluir de forma explícita eventos de risco específicos relacionados à computação em nuvem, tais como: uso indevido de credenciais, vazamento e perda de dados, exploração de vulnerabilidades, falhas na detecção de incidentes, transferência internacional de dados, abusos e ataques a interfaces de programação (API abuse), bem como riscos de lock-in tecnológico e indisponibilidade de serviços. Ressaltou-se que tais eventos demandam tratamento estruturado, considerando impactos operacionais, jurídicos, regulatórios e de segurança da informação.

Também foi debatida a necessidade de corrigir e alinhar as referências normativas e técnicas do Plano de Gestão de Riscos, tendo em vista que o gestor de Segurança da Informação identificou algumas inconsistências de referências no plano atual.

Por fim, o gestor destacou a importância de promover a atualização e revisão de prazos relacionados aos tratamentos de riscos, tendo em vista que alguns já foram executadas e outros precisam de adiamento de prazo para cumprimento da ação, necessitando, portanto, de atualização do cronograma de ações.

A Diretora-Geral lembrou que em reunião anterior a STI disponibilizou o Plano de Gestão de Riscos, assim como os riscos mapeados e seus procedimentos de tratamento em sharepoint compartilhado para os membros do comitê. Após discussões gerais, foram realizadas as seguintes deliberações:

Deliberações:

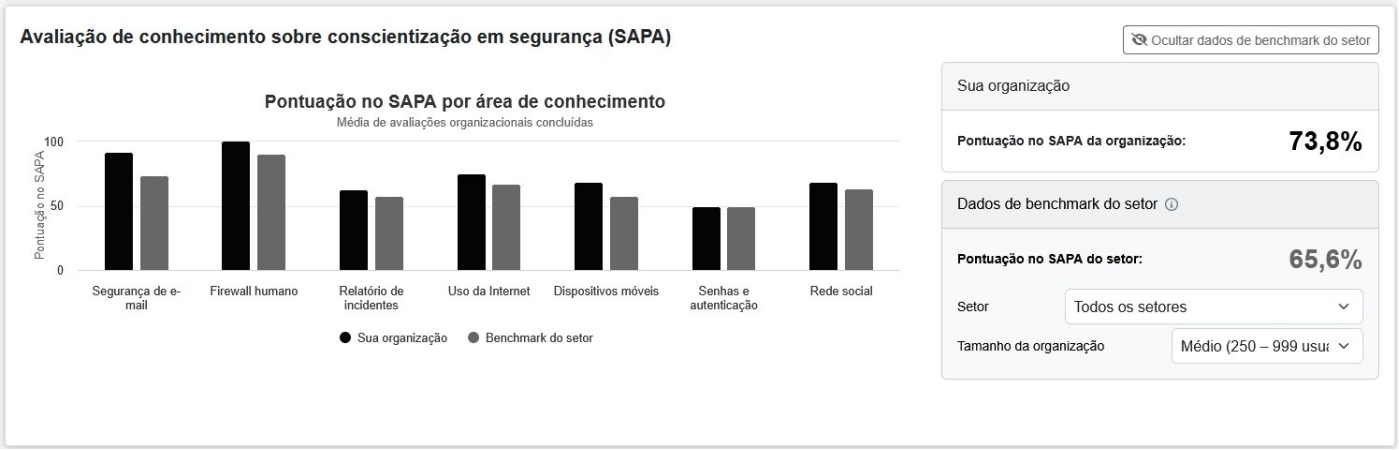
- O Gestor de Segurança da Informação deve realizar as seguintes alterações no Plano de Gestão de Riscos:
  - Inclusão dos riscos ligados a Adoção de Computação em Nuvem, em especial para inclusão e tratamento dos seguintes eventos de riscos:
    - Uso indevido de credenciais
    - Vazamento de dados
    - Perda de dados
    - Exploração de vulnerabilidades
    - Falha em detectar incidentes
    - Transferência internacional de dados
    - Abusos/ataques (API Abuse)
    - Lock-in / indisponibilidade
  - Correção de Referências do Plano de Gestão de Riscos
  - Atualização das ações de controles e de tratamento de riscos, em especial as datas das execuções das iniciativas.
  - Atualização do Cronograma de Ações
- O Gestor de Segurança da Informação deve consolidar os documentos finais com as alterações acima e encaminhá-los para republicação.

Item 5 – Ações de Conscientização e Treinamento Segurança

Apresentação:

O gestor de segurança da informação informou que foi ativado no semestre passado novo relatório da avaliação organizacional da conscientização sobre os diversos aspectos relacionados à Segurança da Informação.

Conforme consta no relatório abaixo, o TRE-AP encontra-se acima da média do benchmark do setor na maior dos tópicos, com exceção de senhas e autenticação. Assim, o gestor recomenda que os usuários continuem participando das campanhas como forma de aumentarmos ainda mais a nossa performance organizacional em relação à S.I



Em relação ao último treinamento de lei geral de proteção de dados, o Gestor de Segurança da Informação constatou baixa adesão dos usuários, recomendando que as áreas fomentem a participação dos servidores nos treinamentos.

Deliberações:

- STI deve reativar o treinamento de LGPD
- STI de reativar o treinamento de S.I
- Os reesposáveis pelas macro-unidades devem fomentar e incentivar os servidores a participarem do treinamento e das campanhas semanais encaminhadas às unidades.

Item 6 – Bloqueio de acesso a dispositivos pessoais e removíveis de armazenamento de dados (Ofício-Circular CNJ nº 313/2025/SG)

Apresentação:

O Gestor de Segurança da Informação informou que o TRE-AP recebeu o Ofício-Circular nº 313/2025/SG (ID SEI 1029264), que informo que devido à 13ª reunião do Comitê Gestor de Segurança da Informação do Poder Judiciário, foi deliberado que os tribunais envidem esforços para o bloqueio do uso de dispositivos pessoais e mídias removíveis de armazenamento de dados, tais como HDs externos, pendrives e dispositivos similares, nas estações de trabalho institucionais.

Citou que a restrição ao uso desses dispositivos visa reduzir riscos associados à introdução de códigos maliciosos, vazamento ou perda de dados, uso indevido de informações institucionais e comprometimento da segurança da informação, alinhando-se às boas práticas de segurança cibernética adotadas no âmbito do Poder Judiciário. O ofício ressaltou, ainda, a recomendação para que seja fomentada a utilização preferencial de diretórios de rede ou soluções em nuvem institucionais, por oferecerem maior nível de segurança, controle de acesso, rastreabilidade, backup automático e sincronização em tempo real, além de favorecerem o compartilhamento seguro de arquivos entre as unidades. Desta forma, o STI opinou que ações fossem tomadas no mesmo sentido neste regional, em alinhamento ao TSE.

Deliberações

- TRE-AP deve manter despacho STI no sentido de prosseguimento de ações para bloqueio de acesso a dispositivos pessoais e removíveis de armazenamento de dados
- STI poderá, em caso excepcionais, como no caso de usos de kits biométricos, não realizar o bloqueio indicado.

Conclusão

Em seguida, o Gestor de Segurança da Informação, Emanoel Flexa, agradeceu a presença de todos e concluiu a reunião.

Documento assinado eletronicamente por **MYLENE LAGES MENDES AZEVEDO**, **Secretário(a)**, em 06/01/2026, às 14:54, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ELINETE NUNES FREITAS**, **Secretário(a)**, em 06/01/2026, às 16:53, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **EMANOEL DOS SANTOS FLEXA**, **Secretário(a)**, em 07/01/2026, às 13:26, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **DILMA CELIA DE OLIVEIRA PIMENTA**, **Diretor(a)-Geral**, em 08/01/2026, às 14:36, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **BRENO BORGES VASCONCELOS DIAS**, **Coordenador(a)**, em 12/01/2026, às 16:57, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **HEVERTON LUIZ RODRIGUES FERNANDES**, **Secretário(a)**, em 14/01/2026, às 13:03, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ADEILSON BATISTA MENDES**, **Assessor(a)**, em 23/03/2026, às 16:22, conforme art. 1º, III, "b", da Lei 11.419/2006.