DIÁRIO DA JUSTIÇA ELETRÔNICO

DO TRIBUNAL REGIONAL ELEITORAL DO AMAPÁ

Ano: 2025, nº 57

Disponibilização: sexta-feira, 28 de março de 2025

Publicação: segunda-feira, 31 de março de 2025

Avenida Mendonça Júnior, 1502 - Centro
Macapá/AP
CEP: 68900-914

Contato
(96) 3198 - 7541
sejud@tre-ap.jus.br

SUMÁRIO

Atos da Presidência 1
Atos da Diretoria-Geral 6
Atos da Secretaria Judiciária 12
Atos da Secretaria de Gestão de Pessoas 21
Atos da 6ª Zona Eleitoral - Santana 22
Atos da 10ª Zona Eleitoral - Macapá / Cutias / Itaubal 23
Índice de Advogados 27
Índice de Partes 27
Índice de Processos 27

ATOS DA PRESIDÊNCIA

PORTARIAS

PORTARIA PRESIDÊNCIA Nº 59/2025 TRE-AP/PRES/ACPRES/ASPRES

Dispõe sobre as regras e os procedimentos para o Gerenciamento de Incidentes de Segurança da Informação do Tribunal Regional Eleitoral do Amapá.

O PRESIDENTE do Tribunal Regional Eleitoral do Amapá (TRE-AP), no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de apoiar o gerenciamento de incidentes de segurança da informação no âmbito do TRE-AP;

CONSIDERANDO a Resolução nº 396/2021 do Conselho Nacional de Justiça (CNJ), que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Resolução nº 23.644/2021 do Tribunal Superior Eleitoral (TSE), que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a Resolução nº 570/2022 do Tribunal Regional Eleitoral do Amapá (TRE-AP), que institui a Política de Segurança da Informação no âmbito da Justiça Eleitoral do Amapá;

CONSIDERANDO a Portaria DG/TSE nº 444/2021, que dispõe sobre a instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral;

CONSIDERANDO as boas práticas de segurança da informação previstas nas normas da Associação Brasileira de Normas Técnicas (ABNT), da *International Organization for Standardization* (ISO) e da *International Electrotechnical Commission* (IEC), notadamente as normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002;

CONSIDERANDO as boas práticas em gestão de incidentes de segurança da informação previstas nas normas ABNT NBR ISO/IEC 27035 (Partes 1, 2 e 3);

CONSIDERANDO as boas práticas de resposta a incidentes previstas no guia *National Institute of Standards and Technology* (NIST) *Special Publication* (SP) 800-61 *Revision* 2;

CONSIDERANDO a Portaria nº 280/2021 do TRE-AP, que institui o Comitê de Crises Cibernéticas;

CONSIDERANDO a necessidade de implementar controles para o tratamento de dados pessoais, nos termos da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);

CONSIDERANDO a Portaria nº 62/2021 do TRE-AP, que institui o Comitê Gestor de Proteção de Dados Pessoais (CGPDP);

CONSIDERANDO a Portaria nº 25/2023 do TRE-AP, que trata dos termos e definições relativos à Política de Segurança da Informação; e

CONSIDERANDO que a segurança da informação e a proteção de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos no âmbito do Tribunal Regional Eleitoral do Amapá,

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Ficam instituídas, por meio desta Portaria, as diretrizes para o gerenciamento de incidentes de segurança da informação no âmbito do Tribunal Regional Eleitoral do Amapá.

Art. 2º Esta Portaria integra a Política de Segurança da Informação do TRE-AP, estabelecida pela Resolução TRE-AP nº 570/2022.

Art. 3º Esta Portaria tem por objetivo descrever as principais estratégias para o tratamento de incidentes computacionais, envolvendo ou não dados pessoais, contemplando as fases de preparação, detecção, contenção, erradicação, recuperação, avaliação e comunicação dos incidentes.

CAPÍTULO II

DAS RESPONSABILIDADES

Art. 4º A atuação operacional na resposta a incidentes de segurança da informação é de responsabilidade da Equipe de Tratamento e Resposta a Incidentes em Redes de Computadores (ETIR), reinstituída pela Portaria Presidência TRE-AP nº 231, de 18 de setembro de 2022.

Art. 5º A comunicação externa com a Autoridade Nacional de Proteção de Dados (ANPD) e com os titulares de dados, nos casos de incidentes graves envolvendo dados pessoais, é de responsabilidade do(a) Encarregado(a) pela Proteção de Dados Pessoais deste Tribunal, designado(a) pela Portaria TRE-AP nº 61, de 26 de março de 2021.

Art. 6º A comunicação externa com a sociedade, em casos de incidentes graves que inviabilizem as atividades essenciais do TRE-AP por período superior ao Objetivo de Tempo de Recuperação (OTR/RTO), é de responsabilidade do Comitê de Crises Cibernética ou de outra autoridade designada pela Presidência do TRE-AP.

Art. 7º Cabe a todas as usuárias e usuários internos comunicar, de forma imediata, a ocorrência ou indícios de incidentes de segurança da informação, por meio dos canais próprios disponibilizados pela Secretaria de Tecnologia da Informação (STI).

Art. 8º Compete ao Comitê de Governança de Segurança da Informação (CGSI) o monitoramento das atividades da ETIR, bem como o estabelecimento de métricas de desempenho relacionadas à resposta a incidentes.

CAPÍTULO III

DA PREPARAÇÃO

Art. 9º A ETIR elaborará seu processo de trabalho e os planos de resposta a incidentes, contendo as etapas do processo de tratamento, conforme os principais tipos de incidentes e ameaças, os quais deverão ficar disponíveis para consulta de seus integrantes.

Art. 10. A Secretaria de Tecnologia da Informação (STI) manterá o registro de *logs* de eventos, conforme regulamentação própria, com o objetivo de subsidiar a detecção manual ou automatizada de incidentes.

Art. 11. A ETIR definirá os meios de comunicação oficiais e adicionais a serem utilizados durante o processo de resposta a incidentes.

Art. 12. A ETIR realizará o monitoramento de ameaças cibernéticas, incluindo o acompanhamento dos boletins encaminhados pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov).

CAPÍTULO IV

DA DETECÇÃO E ANÁLISE

Art. 13. A detecção de incidentes poderá ocorrer por meio de ferramentas automatizadas de monitoramento de eventos, pela análise manual de registros, por comunicação de usuárias e usuários ou pelo monitoramento realizado por operadores técnicos.

Art. 14. Detectado o incidente, ou havendo suspeita de sua ocorrência, a área técnica responsável pelo ativo de informação atingido ou a ETIR deverá realizar o registro do incidente para fins de análise.

Art. 15. Confirmada a ocorrência do incidente, a ETIR acionará o plano de resposta correspondente, conforme a natureza do evento.

Art. 16. As áreas técnicas envolvidas na resposta ao incidente deverão, sempre que possível, atuar para preservar as evidências forenses, visando eventual análise posterior, adotando, entre outras, as seguintes ações:

I - efetuar cópia completa do sistema comprometido;

II - efetuar cópias dos registros de acesso (*logs*);

III - efetuar cópias de mensagens ou arquivos relevantes;

IV - adotar outras medidas previstas no respectivo plano de resposta a incidentes.

CAPÍTULO V
DA CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO
Art. 17. Concluídas as fases de detecção e análise, a ETIR atuará para conter os danos causados pelo incidente, identificar a causa raiz e erradicar a ameaça.
Art. 18. A recuperação do ambiente somente deverá ocorrer após a confirmação de que a ameaça e a vulnerabilidade que originaram o incidente foram devidamente tratadas.
Art. 19. Em caso de incidente classificado como grave, a recuperação do ambiente deverá ocorrer somente mediante autorização do Comitê de Governança de Segurança da Informação (CGSI) ou de outra autoridade designada pela Presidência do TRE-AP.
CAPÍTULO VI
DA AVALIAÇÃO PÓS-INCIDENTE
Art. 20. Concluídas as etapas de tratamento do incidente, a ETIR deverá documentar os procedimentos realizados e as lições aprendidas, por meio da elaboração de relatório de incidente.
Art. 21. O armazenamento dos relatórios de incidentes deverá ocorrer em sistema de informação específico, com acesso restrito aos perfis autorizados.
Art. 22. O registro do incidente de segurança da informação que possa acarretar risco ou dano relevante aos titulares de dados pessoais, nos termos do artigo 48 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), inclusive aqueles não comunicados à ANPD e aos titulares, deverá ser mantido por prazo mínimo de 5 (cinco) anos, contado a partir da data do registro, salvo se houver obrigações adicionais que exijam período superior de guarda.
§ 1º O registro do incidente deverá conter, no mínimo:
I - a data de conhecimento do incidente;
II - a descrição geral das circunstâncias em que o incidente ocorreu;
III - a natureza e a categoria dos dados afetados;
IV - o número estimado de titulares afetados;
V - a avaliação do risco e os possíveis danos aos titulares;
VI - as medidas de correção e mitigação dos efeitos do incidente, quando aplicáveis;
VII - a forma e o conteúdo da comunicação, caso o incidente tenha sido comunicado à ANPD e aos titulares; e
VIII - os motivos da ausência de comunicação, quando for o caso.
§ 2º Os prazos de guarda previstos neste artigo não se aplicam às entidades previstas no artigo 23 da LGPD, desde que observadas as regras específicas aplicáveis aos documentos de guarda permanente, constantes na tabela de temporalidade própria ou definidas pelo Conselho Nacional de Arquivos (CONARQ).
Art. 23. Nos casos em que a causa raiz do incidente não possa ser adequadamente determinada, a ETIR deverá registrá-lo como problema pendente para análise posterior.
CAPÍTULO VII
DA COMUNICAÇÃO
Art. 24. O(a) Gestor(a) de Segurança da Informação apresentará ao Comitê de Governança de Segurança da Informação (CGSI) e ao(à) Coordenador(a) do Comitê Gestor de Proteção de Dados Pessoais (CGPDP) relatório sobre os incidentes que envolvam dados pessoais e que possam acarretar risco ou dano relevante aos titulares, tão logo a gravidade do incidente seja definida.
Art. 25. O(a) Gestor(a) de Segurança da Informação encaminhará ao CGSI relatório resumido de todos os incidentes categorizados como graves.
Art. 26. O(a) Gestor(a) de Segurança da Informação apresentará ao CGSI e à ETIR do Tribunal Superior Eleitoral (TSE) as informações relevantes sobre os incidentes graves ocorridos no âmbito do TRE-AP.

Art. 27. A comunicação à Autoridade Nacional de Proteção de Dados (ANPD) de incidente de segurança que possa acarretar risco ou dano relevante aos titulares deverá ocorrer no prazo máximo de 3 (três) dias úteis, contados do conhecimento do evento pela ETIR.

§ 1º O prazo previsto na cabeça deste artigo será contado a partir do momento em que a ETIR tiver conhecimento de que o incidente afetou dados pessoais.

§ 2º A comunicação à ANPD deverá conter, no mínimo, as seguintes informações:

I - descrição da natureza e da categoria dos dados pessoais afetados;

II - número de titulares afetados, com indicação, quando aplicável, do número de crianças, adolescentes ou idosos;

III - medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente, observados os segredos comercial e industrial;

IV - riscos relacionados ao incidente, com identificação dos possíveis impactos aos titulares;

V - justificativa para eventual atraso na comunicação, quando aplicável;

VI - medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;

VII - data da ocorrência do incidente, se possível determiná-la, e a data de seu conhecimento pela ETIR;

VIII - dados do(a) encarregado(a) ou de representante do TRE-AP;

IX - identificação do controlador ou da controladora;

X - identificação do operador ou da operadora, quando aplicável;

XI - descrição do incidente, incluindo a causa principal, se for possível identificá-la;

XII - total estimado de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

§ 3º As informações poderão ser complementadas, de forma fundamentada, no prazo de 20 (vinte) dias úteis, contados da data da comunicação inicial.

§ 4º A comunicação deverá ser realizada por meio do formulário eletrônico disponibilizado pela ANPD.

§ 5º A comunicação deverá ser feita pelo(a) controlador(a), por meio do(a) encarregado(a), acompanhada de documento comprobatório do vínculo contratual, empregatício ou funcional, ou por representante legalmente constituído, com instrumento que comprove os poderes de representação junto à ANPD.

Art. 28. A comunicação ao(à) titular de dados, nos casos de incidente que possa acarretar risco ou dano relevante, deverá ser realizada no prazo de 3 (três) dias úteis, contados do conhecimento de que o incidente afetou dados pessoais, contendo, no mínimo, as seguintes informações:

I - descrição da natureza e da categoria dos dados pessoais afetados;

II - medidas técnicas e de segurança utilizadas para a proteção dos dados;

III - riscos relacionados ao incidente, com identificação dos possíveis impactos aos titulares;

IV - justificativa para eventual atraso na comunicação;

V - medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;

VI - data do conhecimento do incidente de segurança;

VII - contato para obtenção de informações e, quando aplicável, os dados do encarregado.

§ 1º A comunicação aos(às) titulares deverá:

I - utilizar linguagem simples e de fácil compreensão;

II - ocorrer de forma direta e individualizada, sempre que possível identificá-los.

§ 2º Considera-se comunicação direta e individualizada aquela realizada pelos meios usualmente utilizados pelo(a) controlador(a) para contatar o(a) titular, tais como telefone, e-mail, mensagem eletrônica ou correspondência física.

§ 3º Caso a comunicação direta e individualizada seja inviável, ou não seja possível identificar parcial ou integralmente os(as) titulares afetados(as), o(a) controlador(a) deverá realizar a comunicação, no prazo e com as informações previstas na cabeça deste artigo, por meio dos canais de divulgação disponíveis, tais como sítio eletrônico, aplicativos, mídias sociais e canais de atendimento, garantindo ampla visibilidade por, no mínimo, 3 (três) meses.

§ 4º O(a) controlador(a) deverá incluir, no processo de comunicação, declaração de que a comunicação aos(às) titulares foi realizada, indicando os meios utilizados, no prazo de até 3 (três) dias úteis contados do término do prazo previsto na cabeça deste artigo.

§ 5º Poderá ser considerada boa prática, para os fins do disposto no artigo 52, § 1º, IX, da LGPD, a inclusão, na comunicação ao(à) titular, de recomendações destinadas a reverter ou mitigar os efeitos do incidente.

CAPÍTULO VIII

DAS DISPOSIÇÕES FINAIS

Art. 29. Os casos omissos serão resolvidos pelo Comitê de Governança de Segurança da Informação (CGSI) ou pelo Comitê Gestor de Proteção de Dados Pessoais (CGPDP), conforme a natureza do incidente.

Art. 30. O descumprimento injustificado desta Portaria deverá ser comunicado e registrado pelo Comitê de Governança de Segurança da Informação, com a consequente adoção das providências cabíveis.

Art. 31. Esta Portaria complementar deverá ser revisada anualmente a cada 24 (vinte e quatro) meses, pelo Comitê de Governança de Segurança da Informação.

Art. 32. Esta Portaria entra em vigor na data de sua publicação.

Documento assinado eletronicamente por CARMO ANTONIO DE SOUZA, Presidente, em 26/03/2025, conforme art. 1º, III, "b", da Lei 11.419/2006.

ATOS DA DIRETORIA-GERAL

PORTARIAS

PORTARIA DIRETORIA-GERAL Nº 47/2025 TRE-AP/PRES/DG/SGP/COPES/SRFD

A DIRETORA-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO AMAPÁ, no uso das atribuições legais, e

Considerando o que consta no Processo SEI nº 0000703-23.2025.6.03.8000

RESOLVE:

Art. 1º Comunicar o deslocamento do Excelentíssimo Senhor Juiz Membro do Tribunal Regional Eleitoral do Amapá, para participar da 3ª Edição do Curso Os Desafios da Democracia no Século XXI . Concedendo-lhe diárias conforme regulamentação vigente.

Nome	Cargo	Destino	Saída	Retorno
Jucélio Fleury Neto	Juiz Membro do TRE/AP	São Paulo-SP	30/03/2025	05/04/2025

Art. 2º Publique-se e registre-se.

Documento assinado eletronicamente por DILMA CELIA DE OLIVEIRA PIMENTA, Diretor(a)-Geral, em 26/03/2025, às 15:57, conforme art. 1º, III, "b", da Lei 11.419/2006.