TRIBUNAL REGIONAL ELEITORAL DO PARA

INSTRUÇÃO NORMATIVA Nº 10, DE 07 MAIO DE 2025

Dispõe sobre as regras e os procedimentos para a gestão de incidentes de segurança da informação no âmbito do Tribunal Regional Eleitoral do Pará.

O DIRETOR-GERAL SUBSTITUTO DO TRIBUNAL REGIONAL ELEITORAL DO PARÁ, no uso de suas atribuições legais e regimentais;

CONSIDERANDO a necessidade de estruturar e fortalecer os mecanismos de gestão de incidentes de segurança da informação no TRE do Pará;

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

CONSIDERANDO a Resolução TSE nº 23.644/2021, que institui a Política de Segurança da Informação no âmbito da Justiça Eleitoral;

CONSIDERANDO a Portaria DG/TSE nº 444/2021, que estabelece termos e definições relacionados à Política de Segurança da Informação da Justiça Eleitoral;

CONSIDERANDO a Resolução TRE/PA nº 5.734, de 7 de julho de 2022, que implementa a PSI da Justiça Eleitoral no âmbito deste Regional;

CONSIDERANDO a Portaria nº 20.718/2021 - TRE/PA, que institui o Comitê de Crises Cibernéticas e o Protocolo de Gerenciamento de Crises Cibernéticas;

CONSIDERANDO a Resolução TRE/PA nº 5.699/2021, que institui a Política Geral de Privacidade e Proteção de Dados Pessoais (PGPPD), em consonância com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD);

CONSIDERANDO as boas práticas previstas nas normas técnicas ABNT NBR ISO/IEC 27001, 27002 e 27035 (Partes 1, 2 e 3), e no guia NIST SP-800-61 rev.2;

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Instrução Normativa que disciplina os procedimentos para a gestão de incidentes de segurança da informação no âmbito do Tribunal Regional Eleitoral do Pará.

Art. 2º Esta norma integra a Política de Segurança da Informação da Justiça Eleitoral, conforme estabelecido na Resolução TSE nº 23.644/2021.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 3º Para os efeitos desta Instrução Normativa, aplicam-se os termos definidos na Portaria DG/TSE nº 444/2021, além dos seguintes:

I - ANPD – Agência Nacional de Proteção de Dados Pessoais.

II - CTIR GOV – Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo.

III - ETIR (Equipe Técnica de Respostas a Incidentes de Redes Computacionais ou Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética) – Equipe de tecnologia da informação, de constituição multidisciplinar, coordenada por um Agente Responsável.

IV - Gestor de Segurança da Informação: autoridade responsável pelas ações de segurança da informação e comunicações no âmbito de um órgão ou entidade. Esta função essencial é designada a um servidor público ocupante de cargo efetivo, com formação ou capacitação técnica compatível com as normas estabelecidas, possuindo amplo conhecimento dos processos de negócio do Tribunal e do tema Segurança da Informação.

V - Evento de segurança da informação: Alguma mudança de estado em algum ativo ou serviço de TI, como troca de uma senha, log de acesso a um serviço web, bloqueio da execução de um aplicativo pelo antivírus etc.

VI - Incidente de segurança da informação: Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de informação ou das redes de computadores.

VII - Incidente de segurança da informação com dados pessoais: Qualquer incidente de segurança à proteção de dados pessoais, sendo acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou qualquer forma de tratamento de dados ilícita ou inadequada, que tem a capacidade de pôr em risco os direitos e as liberdades dos titulares dos dados pessoais.

VIII - Incidente grave – Incidente de segurança da informação de maior impacto para a organização, que prejudica de forma intensa a utilização dos serviços de TI ou expõe dados de forma indevida, devendo ser priorizado em relação aos demais incidentes.

IX - Objetivo de Tempo de Recuperação (OTR/RTO) – Período de tempo gasto pela organização para recuperar uma atividade ou processo crítico após sua interrupção, que será definido em portaria específica.

X - Resposta a incidentes: Ação tomada para proteger e restaurar as condições operacionais dos sistemas de informação e as informações neles armazenadas, quando ocorre um ataque ou intrusão.

CAPÍTULO III

DAS RESPONSABILIDADES

Art. 4º A atuação operacional na resposta a incidentes de segurança da informação será de responsabilidade da ETIR – Equipe Técnica de Resposta a Incidentes de Redes Computacionais –, a ser formalmente designada por meio de portaria específica.

§1º Compete à ETIR definir procedimentos técnicos, controles operacionais e fluxos de trabalho voltados à gestão de incidentes de segurança da informação.

§2º A ETIR deverá, ainda, assessorar tecnicamente a Comissão de Segurança da Informação (CSI) e a Secretaria de Tecnologia da Informação (STI) nas análises e deliberações relativas ao tema.

Art. 5º A comunicação externa com a Autoridade Nacional de Proteção de Dados (ANPD), bem como com os titulares dos dados, nos casos de incidentes de segurança considerados graves e que envolvam dados pessoais, será de responsabilidade do Encarregado de Dados Pessoais deste Tribunal, nos termos da Resolução TRE-PA nº 5699/2021.

Art. 6º A comunicação externa com a sociedade, em hipóteses de incidentes graves que comprometam a continuidade dos serviços essenciais prestados pelo TRE do Pará por período superior ao Objetivo de Tempo de Recuperação (OTR/RTO), será de responsabilidade do Secretário de Tecnologia da Informação, ou de outra autoridade que venha a ser designada pela Presidência do Tribunal.

Art. 7º É dever de todos os usuários internos reportar, de forma imediata, quaisquer indícios ou ocorrências de incidentes de segurança da informação dos quais tenham conhecimento, utilizando, para tanto, os canais institucionais disponibilizados pela STI.

CAPÍTULO IV

DA PREPARAÇÃO

Art. 8º Compete à ETIR elaborar e manter atualizados seus processos operacionais e os planos de resposta a incidentes (playbooks), contendo a descrição das etapas a serem executadas conforme os principais tipos de incidentes e ameaças identificados. Esses documentos deverão permanecer disponíveis, em meio seguro, para consulta e uso exclusivo de seus integrantes.

Art. 9º A Secretaria de Tecnologia da Informação deverá manter registros sistemáticos de logs de eventos, em conformidade com a Portaria TRE-PA nº 22.809/2024 – CSI, com a finalidade de subsidiar a detecção, manual ou automatizada, de incidentes de segurança da informação.

Parágrafo único. Os registros mencionados também servirão de base para o monitoramento de métricas e indicadores de desempenho, que visem aferir a eficácia do processo de gestão de incidentes. Exemplos de indicadores incluem, mas não se limitam a: total de incidentes criados, concluídos e em aberto, por status, prioridade ou categoria; tempo médio de reparo; percentual de incidentes solucionados no primeiro atendimento; e percentual de encerramentos dentro do prazo estabelecido.

CAPÍTULO V

DA DETECÇÃO E ANÁLISE

Art. 10. A fase de detecção e análise tem início com a identificação de um possível incidente de segurança da informação, seja este confirmado ou apenas suspeito. O registro da ocorrência deverá ser realizado pela área técnica responsável pelo ativo de informação afetado ou pela ETIR, com vistas à análise preliminar da natureza, causas e impactos do evento sobre os sistemas e dados institucionais.

Art. 11. Confirmada a materialidade do incidente, caberá à ETIR acionar o plano de resposta correspondente ao tipo de incidente identificado, observadas as diretrizes previamente estabelecidas.

Art. 12. As áreas técnicas envolvidas deverão, na medida do possível, adotar providências voltadas à preservação das evidências forenses, com o objetivo de subsidiar a investigação técnica e eventual responsabilização. A preservação compreenderá, dentre outras ações:

I – cópia integral do sistema comprometido;

II – cópia dos registros de acesso (logs);

III – cópia de mensagens e arquivos correlatos;

IV – salvaguarda de quaisquer outros elementos técnicos relevantes ao incidente;

V – demais medidas previstas nos planos de resposta específicos aplicáveis.

Art. 13. No curso da análise e investigação técnica, a ETIR ou o grupo solucionador designado deverá adotar, sempre que possível, as seguintes providências:

I – reconstruir a cronologia dos eventos, de forma a compreender a sequência de ações e identificar a causa-raiz;

II – validar o impacto do incidente, inclusive quanto ao número de usuários afetados, recursos comprometidos e repercussões em processos críticos, ajustando a prioridade de tratamento, se necessário;

III – identificar eventos correlatos, como mudanças recentes, intervenções de usuários ou alterações em itens de configuração que possam ter contribuído para o incidente;

IV – delimitar a falha exata e, quando tecnicamente viável, reproduzir o erro para compreensão aprofundada do problema;

V – examinar logs de erro e eventos relacionados aos itens de configuração (ICs) atingidos, bem como outros registros gerados pelos sistemas;

VI – consultar bases de conhecimento disponibilizadas por fabricantes e fornecedores dos ativos tecnológicos envolvidos, buscando informações e soluções adequadas.

Art. 14. Na hipótese de o incidente apresentar indícios de ação maliciosa, é imprescindível assegurar a preservação de toda a cadeia de evidências digitais relacionadas, com vistas à futura apuração administrativa, técnica ou judicial. Nessas situações, o registro deverá ser, imediatamente, encaminhado à Coordenadoria de Gestão da Segurança da Informação (CGSI/STI) para investigação especializada.

CAPÍTULO VI

DA CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

Art. 15. Concluída a fase de detecção e análise, a ETIR deverá atuar com celeridade na contenção dos danos, na identificação da causa raiz e na erradicação da ameaça, adotando medidas para recuperação dos ativos de informação impactados. Entre as ações aplicáveis, destacam-se:

I – isolamento de sistemas ou redes afetadas;
II – desconexão de sistemas comprometidos;
III – desativação de dispositivos extraviados ou em situação de perda/roubo;
IV – alteração de políticas de rede ou bloqueio de tráfego suspeito;
V – desabilitação de serviços vulneráveis ou comprometidos;
VI – remoção de arquivos ou atividades maliciosas associadas ao incidente;
VII – eliminação de métodos de acesso indevido, como contas ou backdoors instalados pelo atacante.

Art. 16. A recuperação do ambiente somente deverá ser iniciada após a confirmação técnica de que a vulnerabilidade explorada e demais causas que originaram o incidente foram completamente tratadas e mitigadas.

Parágrafo único. A restauração do ambiente deverá abranger a recomposição da integridade dos sistemas afetados, o restabelecimento de suas funcionalidades, a aplicação de medidas adicionais de segurança e, quando cabível, a restauração de backups válidos.

Art. 17. Nos casos classificados como incidente grave, a etapa de recuperação do ambiente dependerá de autorização expressa do Gestor de Crises ou de autoridade competente designada pela Presidência do TRE-PA.

CAPÍTULO VII

DA AVALIAÇÃO PÓS-INCIDENTE

Art. 18. Concluído o tratamento do incidente, a ETIR deverá elaborar relatório detalhado contendo os procedimentos executados, os registros técnicos e as lições aprendidas, com vistas à prevenção de ocorrências futuras. O relatório deverá contemplar, entre outros:

I – análise crítica do incidente, com identificação de fragilidades e pontos de melhoria;
II – verificação da eficácia das medidas de contenção e recuperação adotadas;
III – proposição de aprimoramentos em políticas, normas e processos afetos à segurança da informação;
IV – compilação de dados estatísticos e métricas relevantes para monitoramento contínuo;
V – identificação de elementos necessários a eventuais medidas administrativas ou legais;
VI – registro do feedback dos usuários e partes envolvidas;
VII – atualização de procedimentos internos com base nas conclusões do incidente.

Art. 19. Os relatórios de incidentes deverão ser armazenados em sistema de informação específico, com acesso restrito às áreas competentes.

Art. 20. Quando não for possível determinar a causa raiz do incidente, a ETIR deverá registrá-lo como problema técnico para análise posterior, nos termos dos processos de gerenciamento de problemas.

CAPÍTULO VIII

DA COMUNICAÇÃO

Art. 21. A ETIR deverá encaminhar à Comissão de Segurança da Informação e ao Encarregado de Dados Pessoais relatório sintético de todos os incidentes classificados como graves e que envolvam dados pessoais, tão logo confirmada sua criticidade.

Art. 22. O Gestor de Segurança da Informação apresentará à Comissão de Segurança da Informação e à ETIR do Tribunal Superior Eleitoral os dados relevantes dos incidentes graves ocorridos no âmbito do TRE-PA.

Art. 23. Em situações que envolvam dados pessoais, o Encarregado de Dados Pessoais deverá realizar a comunicação tempestiva à ANPD e aos titulares afetados, conforme definido no plano de comunicação e nos termos da LGPD.

CAPÍTULO IX

DA CAPACITAÇÃO DA EQUIPE DE SEGURANÇA

Art. 24. A Secretaria de Tecnologia da Informação deverá manter programa contínuo de capacitação para os integrantes da ETIR e para os Gestores de Segurança da Informação, contemplando os conhecimentos, habilidades e práticas inerentes ao ciclo de gestão de incidentes de segurança da informação. O conteúdo deverá incluir:

I – etapas da gestão de incidentes: preparação, detecção, análise, contenção, erradicação, recuperação e avaliação;
II – técnicas para identificação, classificação, priorização e análise de incidentes;
III – procedimentos para contenção, erradicação e restauração de serviços afetados;
IV – fundamentos de preservação de evidências digitais e investigação forense;
V – métodos de análise de causa raiz e registro de lições aprendidas;
VI – canais e protocolos de comunicação interna e externa, inclusive com entes reguladores;
VII – utilização de planos de resposta (playbooks) e instruções técnicas padronizadas;
VIII – integração com demais processos de gestão de serviços de TI;
IX – ferramentas de registro e controle, como sistemas de GSTI e bases de conhecimento;
X – gestão específica de incidentes envolvendo dados pessoais e implicações legais.

Parágrafo único. O programa de capacitação deverá prever, sempre que possível, a realização de exercícios simulados com periodicidade mínima anual, visando garantir a prontidão das equipes envolvidas.

CAPÍTULO X

DAS DISPOSIÇÕES FINAIS

Art. 25. Os casos omissos serão resolvidos pelo Comitê Gestor de Segurança da Informação ou, conforme a matéria, pelo Comitê Gestor de Proteção de Dados Pessoais.

Art. 26. O descumprimento injustificado desta Instrução Normativa deverá ser comunicado pelo Gestor de Segurança da Informação à instância competente, para fins de adoção das providências cabíveis.

Art. 27. Esta norma deverá ser revisada, no mínimo, a cada 12 (doze) meses, pela Comissão de Segurança da Informação, com apoio da ETIR.

Art. 28. Esta Instrução Normativa entra em vigor na data de sua publicação, com implementação imediata.

Belém, 07 de maio de 2025.

Documento assinado eletronicamente por **FELIPE HOUAT DE BRITO**, **Diretor-Geral substituto**, em 07/05/2025, às 14:41, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pa.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2692767** e o código CRC **F6FC71E2**.