TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
GABINETE DA PRESIDÊNCIA

PORTARIA Nº 236/2023 – GP

Dispõe sobre a gestão de incidentes de segurança da informação do Tribunal Regional Eleitoral do Rio Grande do Norte.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE, no uso das atribuições que lhe são conferidas pelo artigo 20, inciso XIX, da Resolução nº 09/2012 - TRE/RN, e

CONSIDERANDO a necessidade de apoiar a gestão de incidentes de segurança da informação do Tribunal Regional Eleitoral do Rio Grande do Norte;

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 dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

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

CONSIDERANDO a Resolução TRE/RN nº 110/2023, que institui a Política de Segurança da Informação (PSI) no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte;

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

CONSIDERANDO as boas práticas de resposta à incidentes previstas no guia NIST SP-800-61 rev.2;

CONSIDERANDO a necessidade de gerenciar os incidentes de segurança da informação que envolvam dados pessoais, de acordo com a Lei nº 13.709/2018 (LGPD);

CONSIDERANDO que a segurança da informação e a proteção de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos do Tribunal Regional Eleitoral do Rio Grande do Norte, e tendo em vista o que consta no Processo PAE nº 10.487/2023;

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º A gestão de incidentes de segurança da informação, no âmbito do Tribunal, observará as disposições contidas nesta portaria.

Art. 2º Esta norma integra a Política de Segurança de Informação da Justiça Eleitoral, estabelecida pela Resolução TSE 23.644/2021.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para efeitos desta norma consideram-se os termos e definições previstos 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 de Tratamento e Resposta a Incidentes de Segurança Cibernética): Equipe de tecnologia da informação, de constituição multidisciplinar, coordenada por um Agente Responsável.

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

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

VI - 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.

VII - 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.

VIII - 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.

IX - 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 DISPOSIÇÕES GERAIS

Art. 4º Esta norma tem como objetivo estabelecer diretrizes para as estratégias de gestão de incidentes de segurança da informação, que envolvam ou não dados pessoais, permitindo adequada preparação, detecção, contenção, erradicação, recuperação, avaliação e comunicação no tratamento de incidentes.

Parágrafo único. A gestão de incidentes visa proteger a organização, minimizando os impactos causados por incidentes e apoiando a recuperação rápida do ambiente.

CAPÍTULO IV
DAS RESPONSABILIDADES

Art. 5º A atuação operacional na resposta a incidentes é de responsabilidade da ETIR (Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética), que será nomeada em portaria específica.

Art. 6º A comunicação externa com a ANDP e com os titulares de dados, em caso de incidentes graves envolvendo dados pessoais, é de responsabilidade do Encarregado de Dados Pessoais.

Art. 7º A comunicação externa com a sociedade, em caso de incidentes graves, que inviabilizem as atividades precípuas do TRE/RN por prazo maior que o Objetivo de Tempo de Recuperação (OTR/RTO), é do Gestor de Crises, nomeado em portaria específica, ou por outra autoridade determinada pela presidência do TRE/RN.

Art. 8º Cabe a todos os usuários internos a comunicação imediata caso tenham a informação da ocorrência de quaisquer incidentes de segurança da informação, utilizando os canais próprios fornecidos pela STIE.

Art. 9º Cabe à Comissão Permanente de Segurança da Informação (CPSI) o monitoramento das atividades da ETIR e o estabelecimento de métricas de desempenho.

CAPÍTULO V
DA PREPARAÇÃO

Art. 10. A ETIR elaborará o seu processo de trabalho e planos de resposta à incidentes, contendo os passos do processo de resposta, de acordo com os principais tipos de incidentes e ameaças, os quais ficarão disponíveis para consulta dos seus componentes.

Art. 11 A STIE manterá registro de logs de eventos, de acordo com norma específica, com intuito de subsidiar a detecção manual ou automatizada de incidentes

Art. 12. A ETIR determinará os meios de comunicação oficiais e adicionais a serem acionados durante o processo de resposta à incidentes.

Art. 13. A ETIR fará o monitoramento de ameaças cibernéticas, incluindo o acompanhamento de boletins encaminhados pelo CTIR GOV.

CAPÍTULO VI
DA DETECÇÃO E ANÁLISE

Art. 14. A detecção dos incidentes poderá ocorrer de forma proativa, por meio de sistemas de detecção e prevenção de invasões e ferramentas automatizadas de monitoramento de eventos, pela análise manual de registros de eventos, por comunicação de usuários ou por monitoramento dos operadores técnicos.

Parágrafo único. Os eventos de segurança deverão ser registrados e encaminhados à ETIR para análise.

Art. 15. A ETIR verificará se há a ocorrência de um incidente em potencial e promoverá sua classificação, categorização, correlação e priorização.

§1º Os incidentes devem ser classificados de acordo com a importância ou prioridade das informações e dos sistemas de informações, impacto nos negócios, escala de danos e gravidade.

§2º A priorização do incidente deverá considerar, no mínimo, o seguinte:

I - impacto na imagem da instituição;

II - proteção de informações confidenciais e dados pessoais;

III - ameaça à infraestrutura crítica;

IV - paradas ou danos nas operações.

Art. 16. A ETIR realizará a análise do incidente e sua correlação com outros anteriormente registrados.

Art. 17. As evidências do incidente devem ser preservadas para futura referência ou para procedimentos disciplinares ou legais.

§ 1º A preservação das evidências deve respeitar a cadeia de custódia.

§ 2º Os dados coletados, como arquivo com registro de eventos (log), informação sobre processos, status de conexão de rede, conteúdo de arquivos, software maliciosos, bancos de dados etc., devem ser inscritos em uma imagem como exportação de um banco de dados, arquivo de histórico, captura de tela, imagem de disco, entre outros.

CAPÍTULO VII
DA CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

Art. 18. Após a fase de detecção e análise, A ETIR atuará para conter os danos causados pelo incidente, localizar a causa raiz e erradicar a ameaça, com o objetivo de:

I - parar ou minimizar os efeitos ou danos do ataque, mantendo a continuidade da missão operacional;

II - assegurar a recuperação efetiva e oportuna dos sistemas, de forma a prevenir que incidentes semelhantes ocorram novamente;

III - reforçar a postura defensiva e a prontidão operacional da organização;

IV - assegurar que atividades de resposta ocorram de uma maneira que protejam quaisquer dados, de acordo com o seu nível de sensibilidade;

V - oferecer apoio à caracterização rápida e completa de ataques;

VI - desenvolver e implementar cursos de ação;

VII - remediar ou mitigar a atividade;

VIII - recuperar os sistemas para o nível operacional normal;

IX - melhorar os processos de infraestrutura e de tratamento de incidentes.

Parágrafo único. Antes da execução do procedimento de resposta específico, devem ser coletados todos os dados necessários para a análise e preservação das evidências.

Art. 19. As áreas técnicas envolvidas na resposta ao incidente devem atuar para preservar as evidências forenses para eventual análise posterior, como:

I - efetuar cópia completa do sistema comprometido;

II - efetuar cópias dos logs de acesso;

III - efetuar cópias de mensagens ou arquivos;

IV - outras ações previstas no plano de resposta a incidentes respectivos.

Art. 20. A recuperação do ambiente deve ocorrer somente após a certeza de que a ameaça e a vulnerabilidade que deram causa ao incidente (causa raiz) foram adequadamente tratados.

Art. 21. Em caso de incidente grave, a recuperação do ambiente deve ocorrer somente com aval do Gestor de Crises, ou por outra autoridade determinada pela presidência do TRE/RN.

CAPÍTULO VIII
DA GERAÇÃO DE RELATÓRIOS DE INCIDENTES

Art. 22. O incidente deve ser registrado, especificando quais foram os procedimentos de resposta utilizados para contorná-lo, de forma a manter um histórico das ocorrências e das ações tomadas, considerando o nível de classificação da informação quanto a sua confidencialidade.

Parágrafo único. Registros de incidentes classificados como graves devem ter seu acesso restrito.

Art. 23. A ETIR deverá encaminhar à CPSI o relatório mensal com todos os incidentes ocorridos.

Art. 24. O Agente Responsável pela ETIR encaminhará ao Gestor de Segurança da Informação e ao gestor de crises relatório de todos os incidentes categorizados como graves, tão logo a gravidade do incidente seja definida.

Art. 25. O Agente Responsável pela ETIR encaminhará ao Comitê Gestor de Proteção de Dados Pessoais relatório de todos os incidentes que envolvam dados pessoais.

CAPÍTULO IX
DA COMUNICAÇÃO

Art. 26. O Agente Responsável pela ETIR encaminhará a Comissão Permanente de Segurança da Informação e ao Comitê Gestor de Proteção de Dados Pessoais relatório resumido de todos os incidentes categorizados como graves que envolvam dados pessoais, tão logo a gravidade do incidente seja definida.

Art. 27 O Gestor de Segurança da Informação apresentará à Comissão Permanente de Segurança da Informação e à ETIR do TSE as informações relevantes acerca dos incidentes graves ocorridos.

Art. 28. Em caso de incidentes graves envolvendo dados pessoais, o Comitê Gestor de Proteção de Dados Pessoais informará à ANPD e aos titulares dos dados, de acordo com o plano de comunicação.

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 29. Os casos omissos serão resolvidos pela Comissão Permanente de Segurança da Informação ou pelo Comitê Gestor de Proteção de Dados Pessoais, de acordo com o tipo do incidente.

Art. 30. O descumprimento não fundamentado desta norma deve ser comunicado e registrado pelo Gestor de Segurança da Informação, com consequente adoção das providências cabíveis.

Art. 31 Esta norma complementar deve ser revisada a cada 12 meses pelo Gestor de Segurança da Informação e encaminhada para nova apreciação da Comissão Permanente de Segurança da Informação.

Art. 32. Esta Portaria entra em vigor na data de sua publicação e sua implementação inicia-se imediatamente.

Natal/RN, 12 de dezembro de 2023.

Desembargador **Cornélio Alves**
Presidente