TRIBUNAL REGIONAL ELEITORAL DO CEARÁ

PORTARIA Nº 870/2023

Dispõe sobre a instituição do o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Tribunal Regional Eleitoral do Ceará.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO CEARÁ no uso das atribuições que lhe confere o artigo 23, inciso LX, do Regimento Interno deste Tribunal,

CONSIDERANDO o que dispõe os artigos 7 e 9 da Res. TRE/CE n.º 920/2022, e

CONSIDERANDO o disposto no Processo Administrativo Digital SEI n.º 2023.0.000014518-9,

CONSIDERANDO os termos da Resolução 370, de 28 de janeiro de 2021, do Conselho Nacional de Justiça, que estabeleceu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), as diretrizes para sua governança, gestão e colaboração tecnológica; CONSIDERANDO a Res. CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO o anexo I da Portaria nº 162, de 10 de junho de 2021, do Conselho Nacional de Justiça, que constitui o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário;

CONSIDERANDO os anexos IV, V e VI da Portaria nº 162, de 10 de junho de 2021, do Conselho Nacional de Justiça, que contêm os manuais referentes à Proteção de Infraestruturas Críticas de TIC, Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital, e, ainda, Gestão de Identidades;

CONSIDERANDO a Res. TSE nº 23.644/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

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

CONSIDERANDO as boas práticas de segurança da informação e privacidade previstas nas normas ABNT ISO/IEC 27001 e ABNT ISO/IEC 27002;

CONSIDERANDO a Norma ABNT NBR ISO/IEC 27001:2005, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização;

CONSIDERANDO o Decreto nº 9.637, de 26 de dezembro de 2018, que "Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação";

CONSIDERANDO a Norma Complementar 05/IN01/DSIC/GSIPR, do Gabinete de Segurança Institucional da Presidência da República, de 14 de agosto de 2009, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais (ETIR) nos órgãos e entidades da Administração Pública Federal;

CONSIDERANDO a Norma Complementar 08/IN01/DSIC/GSIPR, do Gabinete de Segurança Institucional da Presidência da República, de 24 de agosto de 2010, que estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal;

CONSIDERANDO o número crescente de incidentes cibernéticos no ambiente da rede mundial de computadores;

CONSIDERANDO as boas práticas de Governança de Tecnologia da Informação para garantir a disponibilidade e integridade dos serviços e ativos tecnológicos do Tribunal Regional Eleitoral do Ceará;

CONSIDERANDO, ainda, que a segurança da informação, a proteção e privacidade de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos do Tribunal Regional Eleitoral do Ceará;

RESOLVE:

Art. 1º Fica instituído o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Tribunal Regional Eleitoral do Ceará.

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

Art. 3º Para efeitos desta norma, consideram-se os termos e definições previstos na Portaria DG /TSE n. 444/2021, além das seguintes:

I. Ativo: qualquer coisa que represente valor para uma instituição, tal como a informação;

II. Ativos de Informação: meios de armazenamento, transmissão e processamento de informação, sistemas de informação e locais onde se encontram esses meios e as pessoas que a eles têm acesso;

III. Atividades críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão, de maneira que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;

IV. Crise: um evento ou série de eventos graves que apresentam propriedades emergentes capazes de exceder as habilidades de uma organização em lidar com as demandas de tarefas que eles geram, e que apresentam implicações que afetam uma proporção considerável da organização, bem como de seus constituintes;

V. Crise Cibernética: crise que ocorre em decorrência de incidente em dispositivos, serviços e redes de computadores, que causam dano material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização;

VI. Evento: qualquer ocorrência observável em um sistema ou rede de uma organização;

VII. Gestão de riscos de segurança da informação: processo que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação e para equilibrá-los com os custos operacionais e financeiros envolvidos;

VIII. Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

IX. Incidente de segurança da informação: evento que viola ou representa uma ameaça iminente de violação de uma política de segurança, de uma política de uso aceitável ou de uma prática de segurança padrão;

X. Processo de gestão de incidentes de segurança da informação: atividades que devem ser executadas para prevenir e tratar a ocorrência de evento adverso de segurança da informação, avaliar o impacto, determinar a resposta inicial e restabelecer a normalidade;

XI. Procedimento: conjunto de ações sequenciadas e ordenadas para o atingimento de determinado fim;

XII. Evidência Digital: informação ou dado, armazenado ou transmitido eletronicamente,

em modo binário, que pode ser reconhecida como parte de um evento;

XIII. Coleta de evidências de segurança em redes computacionais: processo de obtenção de itens físicos que contém potencial evidência, mediante a utilização de metodologia e ferramentas adequadas e inclui a aquisição, ou seja, a geração das cópias das mídias ou a coleção de dados que contenham evidências do incidente;

XIV. Preservação de evidência de incidentes em redes computacionais: é o processo que compreende a salvaguarda das evidências e dos dispositivos para garantir que os dados ou metadados não sofram alteração, preservando-se a integridade e a confidencialidade das informações.

Art. 4º A Secretaria de Tecnologia da Informação e Comunicação (STI) deve incluir no Plano Diretor de TIC (PDTIC) as ações necessárias para adequação dos ativos de tecnologia da informação que suportam as atividades essenciais aos requisitos elencados no Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário.

§1º A lista dos projetos com a inclusão das ações mencionadas no caput deste artigo, deve ser encaminhada à Comissão de Segurança da Informação e ao Comitê de Crises Cibernéticas.

§2º O mesmo tratamento previsto no caput deste artigo deve ser aplicado aos ativos considerados relevantes, mesmo que não estejam diretamente relacionados à sustentação dos serviços críticos que poderiam ser ponto de entrada para a exploração de falhas.

§3º As atividades de Tecnologia da Informação e Comunicação (TIC) essenciais a que se refere o caput deste artigo são as mesmas definidas para o processo vigente de gestão de riscos de tecnologia da informação.

Art. 5º A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR), durante o processo de tratamento do incidente, deve, sem prejuízo de outras ações:

I. Conduzir o tratamento do incidente, observando os procedimentos para coleta e preservação das evidências definidos no Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário, quando constatado ser penalmente relevante;

II. Comunicar o fato à Comissão de Segurança da Informação e ao Comitê de Crises Cibernéticas e à Presidência, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas, considerando o incidente uma crise cibernética;

III. Comunicar o Comitê Gestor de Proteção de Dados do TRE-CE, quando o incidente envolver dados pessoais. Parágrafo único. Cabe ao encarregado(a) pelo tratamento de dados pessoais do TRE-CE comunicar o incidente aos titulares de dados pessoais e, se entender necessário, à Agência Nacional de Proteção de Dados Pessoais (ANPD).

Art. 6º Recebida a comunicação de Incidente de Segurança em Redes Computacionais penalmente relevante, a Presidência deve encaminhá-la ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal, em conjunto com as evidências coletadas.

Art. 7º As ações de coleta e preservação de evidências devem observar o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ), constante do Anexo III da Portaria n. 162, de 2021, do CNJ.

Art. 8º Os casos omissos serão resolvidos pelo Comitê de Segurança da Informação e de Gerenciamento de Crises Cibernéticas.

Art. 9º Qualquer descumprimento desta norma deve ser imediatamente comunicado e registrado pelo Gestor de Segurança da Informação, com consequente adoção das providências cabíveis.

Art. 10º Esta norma complementar deverá ser revisada a cada 12 (doze) meses pelo Comitê de Segurança da Informação e de Gerenciamento de Crises Cibernéticas, sempre que se fizer necessário ou conveniente à este Tribunal.

Art. 11 Esta Política deve ser publicada no portal de intranet do Tribunal pelo Comitê de Segurança da Informação.

Art. 12 Esta Portaria entra em vigor na data de sua publicação.

CIENTIFIQUE-SE, PUBLIQUE-SE E CUMPRA-SE.

Fortaleza, 8 de agosto de 2023.

DESEMBARGADOR RAIMUNDO NONATO SILVA SANTOS

Presidente

Documento assinado eletronicamente por **RAIMUNDO NONATO SILVA SANTOS**, **DESEMBARGADOR PRESIDENTE**, em 08/08/2023, às 10:35, conforme horário oficial de Brasília, com fundamento no art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tre-ce.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=0320482&crc=07C888C7, informando, caso não preenchido, o código verificador **0320482** e o código CRC **07C888C7**.