



TRIBUNAL REGIONAL ELEITORAL DO ACRE

PORTARIA PRESIDÊNCIA Nº 163/2023 PRESI/GAPRES

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO ACRE, DESEMBARGADOR FRANCISCO DJALMA, no uso de suas atribuições legais e regimentais, destacando-se, neste particular, as disposições do Art. 19, XLVI, XLIX e LV do Regimento Interno e,

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

TENDO EM VISTA o anexo III da Portaria nº 162, de 10 de junho de 2021, do Conselho Nacional de Justiça, que aprovou o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ);

TENDO EM VISTA os anexos IV, V e VI da Portaria nº 162/2021, 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 e Controle de Acessos*;

TENDO EM VISTA os termos da Resolução CNJ nº 370/2021, que Instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

TENDO EM VISTA a Norma ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização;

TENDO EM VISTA a Norma ABNT NBR ISO/IEC 27002:2022, que trata de princípios e diretrizes gerais para a Gestão da Segurança da Informação;

TENDO EM VISTA o número crescente de incidentes cibernéticos no ambiente da rede mundial de computadores e a necessidade de processos de trabalho orientados para a boa gestão da segurança da informação;

TENDO EM VISTA as boas práticas de Governança de Tecnologia da Informação e Comunicação (TIC) que visam garantir a disponibilidade e integridade dos ativos tecnológicos deste Tribunal;

TENDO EM VISTA que os ataques cibernéticos têm se tornado cada vez mais avançados e com alto potencial de prejuízo, cujo alcance e complexidade não têm precedentes, que os impactos financeiros, operacionais e de reputação podem ser imediatos e significativos, e que é fundamental aprimorar a capacidade da instituição de estabelecer procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de Polícia Judiciária com atribuição para o início da persecução penal;

TENDO EM VISTA o regramento da Política de Segurança da Informação - Resolução n. 1.776/2022 deste Tribunal Regional Eleitoral do Acre;

TENDO EM VISTA o disposto no processo SEI 0000987-56.2023.6.01.8000,

RESOLVE:

Art. 1º Instituir o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Tribunal Regional Eleitoral do Acre, nos termos deste ato.

Art. 2º O Protocolo de Investigação para Ilícitos Cibernéticos tem por finalidade estabelecer os procedimentos básicos para coleta e preservação de evidências, bem como para comunicar fatos penalmente relevantes aos órgãos de investigação e com atribuição para o início da persecução penal.

Art. 3º Para os efeitos deste normativo, são estabelecidas as seguintes definições:

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

II - Comissão de Segurança da Informação - CSI: equipe multidisciplinar, subordinada à Presidência, com responsabilidade de deliberar, conduzir e fiscalizar as ações de segurança da informação no TRE-AC;

III - Crise: um evento ou série de eventos danosos que apresentam propriedades emergentes capazes de exceder as habilidades de uma organização em lidar com as demandas de tarefas geradas e que apresentam implicações que afetam uma proporção considerável da organização, bem como de seus constituintes;

IV - Crise cibernética: crise que ocorre em decorrência de incidentes em dispositivos, serviços e redes de computadores, que causam danos material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização;

VI - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR: denominação tradicionalmente atribuída a grupos de resposta a incidentes de segurança da informação, embora os incidentes não mais se limitem à tecnologia;

VII - Gerenciamento de crise: decisões e atividades coordenadas que ocorrem em uma organização durante uma crise, incluindo crises cibernéticas;

VIII - Incidente de segurança: evento que viola ou representa ameaça iminente de violação da política de segurança, da política de uso dos recursos de TIC ou de prática de segurança padrão;

IX - Segurança cibernética: é um conjunto de práticas que protege informação armazenada em dispositivos computacionais (computadores, dispositivos móveis, etc) e transmitida através de redes de comunicação, incluindo a Internet e redes de telefonia celular;

X - Segurança da Informação: refere-se a medidas que visam a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, incluindo a preservação da disponibilidade, da confidencialidade e da integridade das informações e dos sistemas. Enquanto a Segurança Cibernética se aplica a uma parte da segurança da informação com foco na proteção digital, cuidando das ameaças às informações transportadas por meios cibernéticos, a Segurança da Informação tem um foco mais amplo, cuidando da redução de riscos no transporte de dados por qualquer meio, seja digital ou não;

Art. 4º No que se refere aos ativos de informação que suportam os serviços essenciais, a Secretaria de Tecnologia da Informação - STI deverá elaborar um relatório de adequação aos requisitos previstos no Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ), constante do Anexo III da Portaria n. 162, de 2021, do CNJ, contendo, no mínimo:

I - a situação de cada requisito (atendido, não atendido ou atendido parcialmente);

II - a aplicabilidade dos requisitos no ambiente tecnológico do TRE-AC;

III - a possibilidade de atendimento e, nesta hipótese, a proposição de prazo de adequação;

IV - a necessidade de capacitação e da aquisição de softwares para implementação dos requisitos dos ativos e das práticas de coleta e de preservação de evidências;

V - a informação quanto à possibilidade da adoção de tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de informação e de ações de usuários, que permita automatizar ações de segurança e oferecer inteligência à análise de eventos de segurança.

§ 1º O relatório citado no caput deste artigo deverá ser encaminhado à Comissão de Segurança da Informação no prazo de 120 (cento e vinte) dias, contado da publicação deste ato.

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

Art. 5º À Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, durante o processo de tratamento do incidente, sem prejuízo de outras ações, compete:

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 - PIILC-PJ (Anexo III da Portaria n. 162, de 2021, do CNJ), quando constatado ser penalmente relevante;

II - comunicar o fato à Comissão de Segurança da Informação;

III - comunicar ao Encarregado(a) pelo Tratamento de Dados Pessoais do TRE-AC, quando o incidente envolver dados pessoais.

§ 1º O Encarregado(a) pelo Tratamento de Dados Pessoais do TRE-AC deverá comunicar o incidente aos titulares de dados pessoais que tiverem seus dados vazados e, se entender necessário, à Agência Nacional de Proteção de Dados Pessoais (ANPD).

§ 2º O Comitê de Crise deverá ser sempre acionado quando o incidente for considerado como crise cibernética.

Art. 6º A Presidência encaminhará ao Ministério Público e à Polícia Judiciária toda comunicação de segurança cibernética que seja considerada como possível ilícito criminal.

Art. 7º O protocolo estabelecido nesta portaria será revisto anualmente ou, quando necessário, em menor prazo.

Art. 8º Esta Portaria entra em vigor nesta a data.

Desembargador **FRANCISCO DJALMA**

Presidente

Rio Branco, 20 de julho de 2023.



Documento assinado eletronicamente por **FRANCISCO DJALMA DA SILVA, Presidente**, em 21/07/2023, às 07:36, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site https://sei.tre-ac.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0600302** e o código CRC **DBF3A602**.

0000987-56.2023.6.01.8000

0600302v2