PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DA PARAÍBA
GABINETE DA PRESIDÊNCIA

ATO DA PRESIDÊNCIA Nº 40/2022

Institui o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ) no âmbito do Tribunal de Justiça da Paraíba.

O **PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DA PARAÍBA**, no uso de suas atribuições legais e regimentais;

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

CONSIDERANDO o anexo III da Portaria nº 162, de 10 de junho de 2021, do Conselho Nacional de Justiça, que constitui o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário;

CONSIDERANDO 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 TI, Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital e, ainda, Gestão de Identidades;

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

CONSIDERANDO 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;

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

CONSIDERANDO 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;

CONSIDERANDO as boas práticas de Governança de Tecnologia da Informação (TI) que visam garantir a disponibilidade e integridade dos ativos tecnológicos deste Tribunal;

CONSIDERANDO 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;

CONSIDERANDO o regramento da Política Segurança da Informação deste Tribunal de Justiça do Estado da Paraíba, **RESOLVE:**

Art. 1º Instituir o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ) no âmbito do Tribunal de Justiça da Paraíba 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 - Comitê de Segurança da Informação: equipe multidisciplinar, subordinada à Presidência, com responsabilidade de deliberar, conduzir e fiscalizar as ações de segurança da informação no TJPB;

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; são incidentes que causam danos material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização;

V - ETIR: Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética. Denominação tradicionalmente atribuída a grupos de resposta a incidentes de segurança da informação, embora os incidentes não mais se limitem a tecnologia;

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

VII - Incidente de Segurança: evento que viola ou representa ameaça iminente de

violação da política de segurança, da política de uso dos recursos de TI ou de prática de segurança padrão;

VIII- Segurança Cibernética: é um conjunto de práticas que protege a informação armazenada nos computadores, nos aparelhos de computação e a informação transmitida através das redes de comunicação, incluindo a Internet e telefones celulares;

IX - 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 as 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 Diretoria de Tecnologia da Informação (DITEC) deverá elaborar um relatório de adequação aos requisitos previstos neste protocolo, contendo, no mínimo:

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

II - a aplicabilidade dos requisitos no ambiente tecnológico do TJPB;

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 ao Comitê 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 A Equipe de Tratamento e Resposta a Incidentes Cibernéticos (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, quando constatado ser penalmente relevante;

II - comunicar o fato ao Comitê de Segurança da Informação;

III - comunicar ao encarregado(a) pelo tratamento de dados pessoais do TJPB, quando o incidente envolver dados pessoais.

§ 1º O encarregado(a) pelo tratamento de dados pessoais do TJPB 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 a Polícia Judiciária toda comunicação de segurança cibernética que seja considerada como possível ilícito criminal.

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 Esta Portaria entra em vigor na data de sua publicação.

Gabinete da Presidência do Tribunal de Justiça do Estado da Paraíba, em João Pessoa, assinado e datado digitalmente.

SAULO HENRIQUES DE SA E BENEVIDES:4682483

Assinado de forma digital por SAULO HENRIQUES DE SA E BENEVIDES:4682483
Dados: 2022.09.05 16:24:36 -03'00'

DESEMBARGADOR SAULO HENRIQUES DE SÁ E BENEVIDES
PRESIDENTE DO TRIBUNAL DE JUSTIÇA DA PARAÍBA