RESOLUÇÃO Nº 22, DE 30 DE MAIO DE 2023.

Institui o Protocolo de Gerenciamento de Crises Cibernéticas (PGCC-PJAL), o Protocolo de Prevenção de Incidentes Cibernéticos (PPINC-PJAL) e o Protocolo de Investigação para Ilícitos Cibernéticos (PIILC-PJAL) do Poder Judiciário, no Tribunal de Justiça do Estado de Alagoas.

O TRIBUNAL DE JUSTIÇA DO ESTADO DE ALAGOAS, no uso de suas atribuições legais,

CONSIDERANDO o previsto na Lei Federal nº. 13.709, de 14 de agosto de 2018, que dispõe sobre a Proteção de Dados Pessoais, alterando a Lei Federal nº. 12.965, de 23 de abril de 2014 (Marco Civil da Internet);

CONSIDERANDO o disposto na Resolução CNJ nº 363, de 12 de janeiro de 2021 que estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos Tribunais;

CONSIDERANDO que a Resolução TJAL nº 03/2021 define que compete ao Comitê de Governança de Tecnologia da Informação e Comunicação (CGOVTIC) promover as ações necessárias à elaboração da Política de Segurança da Informação (PSI) em consonância com os objetivos institucionais, da área de TIC e segurança da informação;

CONSIDERANDO a Resolução CNJ nº 396, de 07 de junho de 2021, que institui a estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário;

CONSIDERANDO, finalmente, o que consta no Proc. Adm. nº 2022/14757, bem como o que decidiu o Plenário do Tribunal de Justiça do Estado de Alagoas, em Sessão Administrativa realizada nesta data,

RESOLVE:

Art. 1º Fica instituído o Protocolo do Gerenciamento de Crises Cibernéticas do Poder Judiciário de Alagoas (PGCC-PJAL), o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário de Alagoas (PPINC-PJAL) - Anexo I e o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJAL) - Anexo II, no Tribunal de Justiça do Estado de Alagoas.

Art. 2º Para fins deste normativo considera-se:

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 para 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: 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 decorrente de incidente em dispositivos, serviços e redes de computadores, que causa dano material ou de imagem, atrai a atenção do público e da mídia e foge ao controle direto da organização;

VI – evento: qualquer ocorrência observável num sistema ou rede da organização;

VII – continuidade de Serviços de TIC (Tecnologia da Informação e Comunicação): abordagem que garante a recuperação dos ativos de TIC e a continuidade das atividades críticas ante um desastre, interrupção ou outro incidente maior;

VIII – gestão de riscos de segurança da informação: processo que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar riscos nos ativos de informação e para equilibrá-los com os custos operacionais e financeiros envolvidos;

IX – gerenciamento de crise: decisões e atividades coordenadas que ocorrem na organização durante crise corporativa, incluindo crises cibernéticas;

X – informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XI – incidente grave: evento que tenha causado dano, colocado em risco ativos críticos de informação ou interrompido a execução de atividades críticas;

XII – incidente de segurança da informação: evento ou série de eventos indesejados ou inesperados de segurança da informação que comprometam ou tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

XIII – processo de gestão de incidentes de segurança da informação: atividades 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; e

XIV – procedimento: conjunto de ações seqüenciadas e ordenadas para atingir um determinado fim.

Art. 3º Fica estabelecido que o Protocolo de Gerenciamento de Crises Cibernéticas (PGCC-PJAL) contempla ações de preparação para lidar com crises cibernéticas. Constituem o PGCC/PJAL os seguintes processos: Processo de Gestão de Riscos de Segurança da Informação, Processo de Monitoramento e Resposta a Incidentes de Segurança da Informação e Processo de Gestão de Continuidade de TIC.

§ 1º São atividades integrantes do Processo de Gestão de Riscos de Segurança da Informação, entre outras:

I - identificar ativos que suportam as atividades críticas, incluindo as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação;

II - avaliar continuamente os riscos a que essas atividades estão expostas; e

III - priorizar o monitoramento, acompanhamento e tratamento dos riscos de maior criticidade.

§ 2º São atividades integrantes do Processo de Monitoramento e Resposta a Incidentes de Segurança da Informação, entre outras:

I - categorizar os incidentes, definindo suas severidades; e

II - estabelecer planos e procedimentos de resposta específicos aos eventuais incidentes, para apoiar equipes em crises cibernéticas.

§ 3º São atividades integrantes do Processo de Gestão de Continuidade de TIC, entre outras:

I - manter os sistemas e serviços críticos de TIC resilientes e em nível operável durante a ocorrência de uma crise, para não interromper a prestação jurisdicional do TJ-AL;

II - elaborar o Plano de Continuidade de TIC para documentar os procedimentos necessários à operação de contingência, bem como o retorno à normalidade, quando ocorrer uma crise pela interrupção dos serviços e sistemas de TIC; e

III - realizar testes periódicos dos planos e análise dos incidentes graves ocorridos, a fim de subsidiar a revisão e melhoria contínua dos processos.

§ 4º O Comitê de Gestão de TIC é responsável por instituir Processo de Gestão de Continuidade de TIC.

Art. 4º Fica instituído o Comitê de Crises Cibernéticas, cujos membros devem ser nomeados por Ato da Presidência, devendo ser composto, no mínimo, por representantes das seguintes áreas:

I - Presidência;
II – Corregedoria-Geral;
III - Comitê Geral de Proteção a Dados Pessoais;
IV - Secretaria-Especial da Presidência;
V - Diretoria de Comunicação;
VI - Diretoria de Tecnologia da Informação;
VII - Direção Geral;
VIII - Procuradoria Geral Administrativa;
IX - Assessoria Militar;
X - Departamento Central de Aquisições; e
XI - Assessoria de Planejamento - APMP.

Parágrafo único. A coordenação do Comitê de Crises Cibernéticas ficará a cargo do Presidente do TJ-AL.

Art. 5º São atribuições do Comitê de Crises Cibernéticas:

I – entender claramente o incidente que gerou a crise, sua gravidade e os impactos negativos;

II – levantar todas as informações relevantes;

III – levantar soluções alternativas para a crise, apreciando sua viabilidade e suas consequências;

IV – avaliar a necessidade de suspender serviços e/ou sistemas informatizados;

V – centralizar a comunicação na figura de um porta-voz para evitar informações equivocadas ou imprecisas;

VI – aplicar o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário;

VII – avaliar a necessidade de recursos adicionais extraordinários para apoiar as equipes de resposta;

VIII– fornecer aconselhamento sobre as prioridades e estratégias da organização para uma recuperação rápida e eficaz;

IX – elaborar plano de retorno à normalidade;

X – aplicar o Protocolo de Prevenção de Incidentes Cibernéticos.

Art. 6º Em caso de interrupção dos serviços de TIC por tempo maior do que aquele definido em ato próprio para cada serviço essencial, às atividades desempenhadas pela organização e suportadas por estes serviços de TIC poderão ser interrompidas até o restabelecimento da normalidade, sendo o Comitê responsável por gerenciar esse procedimento.

Art. 7º O CCC dever-se-á se reunir na sala de situação trimestralmente ou sempre que for necessário.

Parágrafo único. A sala de situação deve-se constituir em ambiente reservado que viabilize o equilíbrio às deliberações, devendo dispor de recursos materiais e humanos especialmente destacados para a execução de atividades administrativas durante o período de crise.

Art. 8º Em caso de ocorrência de incidente que gere ou possa gerar crise cibernética, o Comitê de Crises deve ser imediatamente comunicado e convocado para reunião.

§ 1º Caso seja confirmada a crise cibernética, o Comitê de Crises Cibernéticas entrará em estado de convocação permanente, podendo reunir-se a qualquer horário para discutir, deliberar e agir no tratamento da crise em curso.

§ 2º O acesso às reuniões do Comitê de Crises Cibernéticas deve ser restrito aos membros do Comitê e a atores eventualmente convidados.

Art. 9º As ações de resposta e recuperação da crise cibernética devem observar o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCC-PJ).

Art. 10º Este Ato entra em vigor a partir da data de sua publicação.

Desembargador FERNANDO TOURINHO DE OMENA SOUZA
Presidente do Tribunal de Justiça de Alagoas

Desembargador OTÁVIO LEÃO PRAXEDES

Desembargador ALCIDES GUSMÃO DA SILVA

Desembargador TUTMÉS AIRAN DE ALBUQUERQUE MELO

Desembargador KLEVER RÊGO LOUREIRO

Desembargador PAULO BARROS DA SILVA LIMA

Desembargador JOÃO LUIZ AZEVEDO LESSA

Desembargador FÁBIO JOSÉ BITTENCOURT ARAÚJO

Desembargador DOMINGOS DE ARAÚJO LIMA NETO

Desembargador CELYRIO ADAMASTOR TENÓRIO ACCIOLY

Desembargador CARLOS CAVALCANTI DE ALBUQUERQUE FILHO

Desembargador ORLANDO ROCHA FILHO

Desembargador IVAN VASCONCELOS BRITO JÚNIOR

Desembargador FÁBIO COSTA DE ALMEIDA FERRARIO

Disponibilzado no Diário da Justiça Eletrônico em 01/06/2023.
Págs. 107 302

ANEXO I – Protocolo – Prevenção de incidentes cibernéticos do PoderJudiciário de Alagoas

Protocolo

Prevenção de Incidentes Cibernéticos do Poder Judiciáriode Alagoas

Material de referência com as principais diretrizes necessárias para implantação doprotocolo de prevenção de incidentes cibernéticos do Poder Judiciário

PODER JUDICIÁRIO DE ALAGOAS

Sumário

Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário(PPINC-PJ)

1. Escopo

O Protocolo de Prevenção a Incidentes Cibernéticos contemplará um conjunto de diretrizes para a prevenção a incidentes cibernéticos em seu mais alto nível.

As diretrizes serão divididas em funções que expressem a gestão do risco organizacional e que permitam as decisões adequadas para o enfrentamento de ameaçase a melhor gestão de práticas e de metodologias existentes.

2. Funções básicas

São funções básicas do Protocolo de Prevenção a Incidentes Cibernéticos: identificar, proteger, detectar, responder e recuperar, nos seguintes termos.

identificar: entendimento organizacional para gerenciar o risco de ataques cibernéticos a sistemas, pessoas, ativos, dados e recursos. Permite ao órgão avaliar os recursos que suportam funções críticas e os riscos relacionados. São medidas de concentração e priorização dos esforços na gestão de ativos, ambiente de negócios, governança, avaliação de riscos e estratégia de gestão deriscos.

proteger: desenvolvimento e implementação de salvaguardas que assegurem a proteção de dados, inclusive pessoais, de ativos de informação; e a prestação de serviços críticos. Possibilita aos órgãos suportar e conter impactos ocasionados por incidentes cibernéticos. Nessa função, estão incluídas as seguintes medidas, sem prejuízo de outras eventualmente adotadas: gerenciamento de identidade e controle de acesso, conscientização e treinamento, segurança de dados, processos e procedimentos de proteção da informação, medidas de atualização, manutenção e tecnologias de proteção.

detectar: desenvolvimento e implementação de atividades adequadas à descoberta oportuna de eventos ou à detecção de incidentes de segurança

cibernética. Estão contempladas ações de monitoramento contínuo de segurança,processos de detecção de anomalias e eventos.

responder: desenvolvimento e implementação de atividades apropriadas à adoção de medidas em incidentes cibernéticos detectados. Nessa categoria, são incluídos os planos de resposta, de comunicações, de análise, de mitigação e demelhorias.

recuperar: desenvolvimento, implementação e manutenção dos planos de resiliência e de restauração de quaisquer capacidades ou serviços que foram prejudicados em razão de incidentes de segurança cibernética.

3. Princípios críticos

base de conhecimento de defesa: consiste no uso de informações e conhecimento de ataques reais que comprometeram sistemas. Informações conseguidas por meio de interação e de cooperação com outras equipes de tratamento a incidentes e respostas. Tem por propósito fornecer bases fundamentais ao aprendizado contínuo com apoio em eventos ocorridos. Apoia a construção de defesas eficazes e práticas.

priorização: foco prioritário na formação, na revisão de controles, nos processose na disseminação da cultura de segurança cibernética. Contribui para a reduçãode riscos e para a proteção contra as ameaças mais sensíveis e que encontram viabilidade em sua célere implementação.

instrumentos de medição e métricas: definição e estabelecimento de métricas comuns que fornecem linguagem compartilhada e de compreensão abrangente para magistrados e magistradas, servidores e servidoras, colaboradores e colaboradoras, prestadores e prestadoras de serviços, especialistas em tecnologia da informação, auditores e demais atores do sistema de segurança. Permite a

medição da eficácia das medidas de segurança dentro da organização. Fornece insumos para que os ajustes necessários, quando identificados, possam serimplementados de forma célere.

diagnóstico contínuo: processo de trabalho que realiza continuamente mediçãopara testar e validar a eficácia das medidas de segurança atuais e contribui para a definição de prioridades e para os próximos passos a serem tomados.

formação e capacitação: processos formais de educação continuada com a inclusão em planos de capacitação que contemplem a disseminação, a formação e a instrução para todos os atores envolvidos em atividades diretas ou indiretas que contribuam para a cultura de segurança cibernética dentro da organização. Tais instrumentos deverão ser revisados periodicamente.

automação: incentivo à busca de soluções automatizadas de segurança cibernética para que as organizações obtenham medições confiáveis, escaláveis e contínuas. Tal processo está correlacionado com os resultados almejados por meio dos instrumentos de controle e de métricas**.**

resiliência: poder de recuperação ou capacidade de a organização resistir aos efeitos de um incidente.

4. Gestão de Incidentes de Segurança da Informação

A gestão de incidentes de segurança da informação é realizada por meio de processo definido e constituída formalmente, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança.

5. Competência de atuação

Deverá ser formalmente instituída Equipe de Tratamento e Resposta a Incidentesde Segurança Cibernética (ETIR).

A ETIR poderá solicitar apoio multidisciplinar que abranja as áreas: tecnologia da informação, segurança da informação, jurídica, pesquisas judiciárias, comunicação, controle interno, segurança institucional, entre outras, necessárias para responder aos

incidentes de segurança de maneira adequada e tempestiva.

Caberá a cada órgão do Poder Judiciário avaliar o adequado posicionamento da ETIR em seu organograma institucional, considerando-se seu desenho organizacional e suas peculiaridades.

A ETIR terá autonomia compartilhada, ou seja, participará do resultado da decisão recomendando os procedimentos a serem executados ou as medidas de recuperação durante a identificação de uma ameaça e debaterá sobre as ações a serem tomadas, seus impactos e a repercussão, caso as recomendações não sejam seguidas.

6. Funcionamento da ETIR

O funcionamento da ETIR é regulado por documento formal de constituição, publicado no sítio eletrônico do respectivo órgão, devendo constar, no mínimo, os seguintes pontos:

a) definição da missão;
b) público-alvo;
c) modelo de implementação;
d) nível de autonomia;
e) designação de integrantes;
f) canal de comunicação de incidentes de segurança; e
g) serviços que serão prestados.

7. Boas Práticas de Segurança Cibernéticas

A segurança cibernética é um empreendimento coletivo.

Para melhor detectar, conter e eliminar ataques cibernéticos e minimizar eventuais impactos na operação, assegurando o funcionamento dos sistemas críticos do Poder Judiciário, sobretudo em ambiente de constante ameaça, é necessário que todos os seus órgãos possuam mecanismos de respostas e prevenção.

A prevenção a incidentes contempla funções de preparação, identificação, contenção, erradicação, recuperação e lições aprendidas.

As dimensões e práticas poderão ser adaptadas, incrementadas ou ajustadas

conforme a realidade de cada órgão.

São assim definidas as dimensões e práticas da segurança cibernética:

preparação: processo que envolve as equipes de tratamento a incidentes e respostas. Trata-se de resposta metódica, contemplando ferramentas forenses de análise e custódia, identificação de cadeia de comando em situação de crise, processos de educação e de formação.

identificação: capacidade de identificar que um ataque cibernético está em andamento, por meio da percepção de sinais de anomalias ou de comportamentos inesperados. Trata-se da aptidão dos entes para diferenciar as irregularidades em redes de dados e identificar o mau funcionamento dos sistemas críticos, em razão de ataques cibernéticos em curso. Para essa atividade, podem ser elaboradas listas de verificação investigativas para apoiar o processo de diagnóstico, triagem e acionamento das equipes de resposta, permitindo a avaliação do impacto e a determinação dos próximos passos a serem tomados.

contenção: visa a garantir que o incidente não cause mais danos, por meio da adoção dos mecanismos de comunicação previstos no Protocolo de Gerenciamento de Crises. Nessa dimensão, a prioridade geral é isolar o que foi afetado, manter a produção e, acima de tudo, garantir que as ações não comprometam, ainda mais, a segurança ou as operações críticas. Tal atividade tende a ser complexa, devendo os utilitários isolar a fonte de um ataque e determinar o momento de aplicação de ferramenta forense passiva construída para remoção de malware das redes de produção ou para a limitação de transferências de dados desnecessárias**.**

erradicação: remoção da ameaça, garantindo que as operações essenciais sejam apoiadas, caso surjam desafios no processo de restauração. Os métodos possíveis para essa função podem variar desde patches ou reconstruções do sistema até redesenho completo da arquitetura, devendo, sempre que possível, preservar evidências que apoiarão o processo de investigação do

crime cibernético.

recuperação: promulgação de plano de recuperação em fases para restauração de operações, com foco prioritário nos sistemas críticos ou na execução da operação em modo analógico até que haja confiança no desempenho do sistema. Nessa atividade, são necessárias verificações ambientais e de segurança paralelas ao controle dos impactos de desempenho não intencionais da restauração.

lições aprendidas: atividade contínua que não só deve capturar os impactos imediatos de um incidente, mas também as melhorias em longo prazo da segurança cibernética do órgão. Tal função pode variar de um sistema de controle de processos melhor projetado até a evolução e preparação de centros de identificação e resposta a ataques cibernéticos do Poder Judiciário.

ANEXO II – Protocolo – Protocolo de Investigação para IlícitosCibernéticos do Poder Judiciário (PIILC-PJ)

Protocolo

Protocolo de Investigação para Ilícitos Cibernéticos do PoderJudiciário (PIILC-PJ)

Material de referência com as principais diretrizes necessárias para implantação do protocolo de prevenção de Investigação para Ilícitos Cibernéticos do Poder Judiciário(PIILC-PJ)

Art. 1º Instituir o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário(PIILC-PJ) no âmbito do Tribunal de Justiça de Alagoas.

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 protocolo, são estabelecidas as seguintes definições:

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

II - Comitê Gestor de Proteção de Dados: equipe multidisciplinar, subordinadaà Presidência, com responsabilidade de deliberar, conduzir e fiscalizar as ações desegurança da informação no TJAL;

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, bemcomo 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 daorganização;

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 (DIATI) 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 TJAL;

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

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 desegurança.

§ 1º O relatório citado no caput deste protocolo deverá ser encaminhado ao Comitê de Segurança da Informação no prazo de 120 (cento e vinte) dias.

§ 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 Gestor de Proteção de Dados;

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

§ 1º O encarregado(a) pelo tratamento de dados pessoais do TJAL 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 Gestor de Proteção de Dados deverá ser sempre acionado quando o incidente for considerado como Crise Cibernética.

Art. 6º A Presidência encaminhará ao Ministério Público e a Polícia Civil toda comunicação de segurança cibernética que seja considerada como possível ilícitocriminal.

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.