TRIBUNAL REGIONAL ELEITORAL DO PARA

PORTARIA Nº 20718/2021 TRE/PRE/DG/GABDG

Institui o Comitê de Crises Cibernéticas e o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Tribunal Regional Eleitoral do Estado do Pará.

A PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO PARÁ , no uso de suas atribuições legais e regimentais, e à vista do que consta no processo SEI nº 0000045-32.2021.6.14.8000;

CONSIDERANDO que é imprescindível garantir a segurança cibernética do ecossistema digital no âmbito do Tribunal Regional do Pará;

CONSIDERANDO os termos da Resolução CNJ n.° 396/2021, que "Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)", estabelecendo uma série de controles mínimos e medidas a serem adotadas pelos órgãos do Judiciário;

CONSIDERANDO os termos do Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário - Anexo II da Portaria CNJ n.º 162 de 10/6/2021, que aprovou os Protocolos e Manuais criados pela Resolução CNJ nº 396/2021;

CONSIDERANDO a necessidade de constituir estruturas organizacionais e estabelecer respostas compatíveis com os níveis de risco, agindo de forma proativa e reativa a incidentes de segurança da informação;

RESOLVE:

Art. 1º Fica instituído o Comitê de Crises Cibernéticas e o Protocolo de Gerenciamento de Crises Cibernéticas no Tribunal Regional Eleitoral do Pará.

§ 1º O Comitê de Crises Cibernéticas (CCCb/TRE-PA) será composto por representantes das seguintes estruturas de governança e unidades do Tribunal Regional Eleitoral, designados por meio de Portaria:

I - Presidência;

II – Corregedoria;

III - Diretoria Geral;

IV - Secretaria Judiciária;

V - Assessoria de Comunicação Institucional;

VI - Secretaria de Tecnologia da Informação;

VII - Comitê Gestor de Proteção de Dados Pessoais (CGPD);

VIII - Comissão de Segurança da Informação (CSI);

IX - Secretaria de Administração; e

X - Gabinete de Segurança Institucional.

§ 2º O Protocolo de Gerenciamento de Crises Cibernéticas no Tribunal Regional Eleitoral do Pará será composto pelas seguintes etapas:

I – Identificação;

II - Fase Preparatória (Pré-crise);

III - Durante a Crise Cibernética;

IV - Melhoria Contínua (Lições aprendidas no Pós-crise).

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 2º Para os efeitos deste normativo, são estabelecidos os seguintes conceitos e definições:

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: um evento ou uma série de eventos danosos 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: decorre de incidentes 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 em uma rede de uma organização;

VII – gerenciamento de crise: decisões e atividades coordenadas que ocorrem em uma organização durante uma crise corporativa, incluindo crises cibernéticas;

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 grave: evento que tenha causado dano, colocado em risco ativo de informação crítico ou interrompido a execução de atividade crítica por um período inferior ao tempo objetivo de recuperação; e

X – incidente de segurança da informação: evento que viola ou representa ameaça iminente de violação de política de segurança, de política de uso aceitável ou de prática de segurança padrão.

CAPÍTULO II
DO COMITÊ DE CRISES CIBERNÉTICAS

Art. 3º O Comitê de Crises Cibernéticas (CCCb/TRE-PA) deverá ser acionado pela Secretaria de Tecnologia da Informação sempre que for identificada uma crise cibernética.

§ 1º O Comitê de Crises Cibernéticas, quando acionado, será coordenado pelo Diretor Geral do TRE-PA.

§ 2º No desempenho de suas atribuições institucionais, o CCCb/TRE-PA deverá observar as diretrizes da Política de Segurança da Informação (PSI) do Tribunal Regional Eleitoral do Pará, definidas em resolução e atuar de forma coordenada com a Comissão de Segurança da Informação (CSI).

§ 3º As deliberações e propostas do CCCb/TRE-PA deverão estar em consonância com os normativos e recomendações do Conselho Nacional de Justiça (CNJ) e do Tribunal Superior Eleitoral (TSE).

§ 4º As deliberações do CCCb/TRE-PA serão motivadas e aprovadas, com registro em Ata em processo no Sistema Eletrônico de Informações - SEI, por maioria simples.

§ 5º A Secretaria de Tecnologia da Informação poderá ser acionada em casos de suspeita de ataque cibernético, por meio do ramal VoiP (91) 3346-8800 - Central de Serviços de TI - Servicedesk.

Art. 4º O Comitê de Crise Cibernéticas deverá coordenar esforços com equipes administrativas e técnicas do TRE-PA objetivando:

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

II - levantar todas as informações relevantes, verificando fatos e descartando boatos;

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 - realizar comunicação tempestiva e eficiente, que evidencie o trabalho diligente das equipes e enfraqueça boatos ou investigações paralelas que alimentem notícias falsas;

VII - definir estratégias de comunicação com a imprensa e/ou redes sociais e estabelecer qual a mídia mais adequada para se utilizar em cada caso;

VIII - determinar que a Equipe de Tratamento de Incidentes de Rede - ETIR/TRE-PA aplique o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário;

IX - solicitar a colaboração de especialistas do TSE ou CNJ, ou de centros de resposta a incidentes de segurança;

X - apoiar equipes de resposta e de recuperação com gerentes de crise experientes;

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

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

XIII – definir os procedimentos de compartilhamento de informações relevantes para a proteção de outras organizações com base nas informações colhidas sobre o incidente; e

XIV – elaborar plano de trabalho de retorno à normalidade.

Art. 5º O Comitê de Crises Cibernéticas se reunirá, ordinariamente, a cada bimestre para a avaliação e monitoramento das ações de segurança cibernética no Tribunal Regional Eleitoral do Pará e, extraordinariamente, sempre que ocorrer incidente.

CAPÍTULO III
DA IDENTIFICAÇÃO DE CRISE CIBERNÉTICA

Art. 6º O gerenciamento de incidentes se refere às atividades que devem ser executadas na ocorrência de evento adverso de segurança da informação, para avaliar o problema e determinar a resposta inicial.

Art. 7º O gerenciamento de crise se inicia quando:

I - o incidente for caracterizado como grave causando dano material ou de imagem;

II - for evidente que um incidente cibernético não poderá ser mitigado rapidamente e que as ações de resposta poderão durar dias, semanas ou meses;

III - o incidente impactar a atividade finalística ou serviço crítico mantido pela organização, provocando a disrupção ou degradação de serviços essenciais; ou

IV - o incidente atrair grande atenção da mídia e da população em geral.

Art. 8º São considerados Incidentes Cibernéticos considerados de severidade alta e crítica, dentre outros:

I - degradação ou interrupção de serviços ou sistemas por ataque de negação de serviço (Denial-of-Service - DoS) (severidade alta);

II - comprometimento de credenciais com acesso a informações sensíveis (severidade alta);

III - importantes informações organizacionais tornam-se inacessíveis devido a processo de encriptação ou ataque por ransomware (severidade crítica);

IV - vazamento de informação e dados pessoais sensíveis (severidade crítica).

CAPÍTULO IV
DA FASE PREPARATÓRIA (PRÉ-CRISE)

Art. 9º Para melhor lidar com uma crise cibernética, o TRE-PA deverá realizar prévia e adequada preparação, mediante instituição do Plano de Continuidade de Serviços Essenciais de TIC, que contemple, no mínimo, as seguintes atividades:

I - observar o Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário, conforme disciplinado pelo Anexo I da Portaria CNJ Nº 162 de 10/06/2021, que aprovou os Protocolos e Manuais criados pela Resolução CNJ nº 396/2021;

II - definir, ou reconhecer, quais são os serviços e sistemas/infraestrutura de apoio considerados essenciais ou que são fundamentais para a atividade finalística do órgão;

III - identificar os ativos de informação críticos, ou seja, aqueles que suportam as atividades primordiais, incluindo as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação;

IV - avaliar continuamente os riscos a que as atividades críticas estão expostas e que possam impactar diretamente na continuidade do negócio;

V - realizar, continuamente, a análise de vulnerabilidades dos ativos de TI essenciais ao negócio;

VI - categorizar os incidentes e estabelecer procedimentos de resposta específicos (playbooks) para cada tipo de incidente, de forma a apoiar equipes técnicas e de liderança em casos de incidentes cibernéticos graves;

VII - priorizar o monitoramento, acompanhamento e tratamento dos riscos de maior criticidade; e

VIII - realizar simulações e testes para validação dos planos e procedimentos.

§ 1º A Secretaria de Tecnologia da Informação e a Comissão Diretiva de TI (CDTI) expedirão os atos que contemplem a concretização do programa de gestão da continuidade de Serviços Essenciais de TIC.

§ 2º As atividades insertas no inciso VII deste artigo deverão ser detalhadas e consolidadas em um plano de contingência que contemple diversos setores em razão de possíveis cenários de crise, a fim de se contrapor à escalada de uma eventual crise e com o objetivo de manutenção dos serviços prestados pela organização.

CAPÍTULO V
DURANTE A CRISE CIBERNÉTICA

Art. 10. O Comitê de Crises Cibernéticas deve coordenar ações para garantir que a comunicação entre as áreas envolvidas em crise seja tratada como fator crítico para que a organização possa responder à crise cibernética de longa duração ou de grande impacto.

Art. 11. Assim que a ETIR/TRE-PA (Equipe de Tratamento de Incidentes de Rede) identificar que um incidente constitui crise cibernética, deverá solicitar imediatamente reunião do Comitê de Crises Cibernéticas.

§ 1° O Comitê de Crises Cibernéticas deve reunir-se presencialmente ou virtualmente, através de tecnologia oficial de videoconferência adotada no Tribunal, para deliberar se o incidente reportado pelo ETIR/TRE-PA constitui crise cibernética.

§ 2° 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.

§ 3° O acesso às reuniões do Comitê de Crises Cibernéticas deve ser restrito aos membros deste Comitê e a atores eventualmente convidados a participar das reuniões.

§ 4° A Assessoria de Comunicação deve auxiliar o representante do Comitê de Crises Cibernéticas no acesso ágil a meios que permitam fazer declarações públicas à imprensa.

§ 5° O Comitê de Crises Cibernéticas deve contar com equipe dedicada à execução de atividades administrativas necessárias durante o período de crise.

Art. 12. Os planos de contingência existentes, caso aplicáveis, devem ser efetivados imediatamente, visando à continuidade dos serviços prestados pelo Tribunal.

Art. 13. Para eficácia do trabalho, deverá o Comitê de Crise:

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

II - levantar todas as informações relevantes, verificando fatos e descartando boatos;

III - levantar soluções alternativas para a crise, avaliando sua viabilidade e 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 - realizar comunicação tempestiva e eficiente, de forma a evidenciar o trabalho diligente das equipes e a enfraquecer boatos ou investigações paralelas que alimentem notícias falsas;

VII - definir estratégias de comunicação com a imprensa e/ou redes sociais e estabelecer qual a mídia mais adequada para se utilizar em cada caso;

VIII - aplicar o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário;

IX - solicitar a colaboração de especialistas ou de centros de resposta a incidentes de segurança;

X - apoiar equipes de resposta e de recuperação com gerentes de crise experientes;

XI - avaliar a necessidade de recursos adicionais extraordinários a fim de apoiar as equipes de resposta;

XII - orientar sobre as prioridades e estratégias da organização para recuperação rápida e eficaz;

XIII - definir os procedimentos de compartilhamento de informações relevantes para a proteção de outras organizações com base nas informações colhidas sobre o incidente; e

XIV - elaborar plano de retorno à normalidade.

Art. 14. As etapas e procedimentos de resposta são diferentes de acordo com o tipo de crise, sendo necessárias reuniões regulares para avaliar o progresso até que seja possível retornar à condição de

normalidade.

CAPÍTULO VI
FASE DE MELHORIA CONTÍNUA (LIÇÕES APRENDIDAS NO PÓS-CRISE)

Art. 15. Após o retorno das operações à normalidade, o Comitê de Crises Cibernéticas, apoiado pela ETIR/TRE-PA, deverá emitir relatório contendo a análise criteriosa das ações tomadas, observando as que foram bem-sucedidas e as que ocorreram de forma inadequada.

Parágrafo único. O Relatório de Comunicação de Incidente de Segurança Cibernética deve conter a descrição e o detalhamento da crise, bem como o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados.

Art. 16. Para a identificação das lições aprendidas e a elaboração de relatório final, deve ser objeto de avaliação:

I - a identificação e análise da causa-raiz do incidente;

II - a linha do tempo das ações realizadas;

III - a escala do impacto nos dados, sistemas e operações de negócios importantes durante a crise;

IV - os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas;

V - o escalonamento da crise;

VI - a investigação e preservação de evidências;

VII - a efetividade das ações de contenção;

VIII - a coordenação da crise, liderança das equipes e gerenciamento de informações; e

IX - a tomada de decisão e as estratégias de recuperação.

Art. 17. As lições aprendidas devem ser utilizadas para a elaboração ou revisão dos procedimentos específicos de resposta (playbooks) e para a melhoria do processo de preparação para crises cibernéticas.

CAPÍTULO VII
DA COMUNICAÇÃO DO INCIDENTE DE SEGURANÇA

Art. 18. Assim que tomar conhecimento de Incidente de Segurança em Redes Computacionais, penalmente relevante, que possa causar a deflagração de uma crise cibernética, o Comitê de Crises Cibernéticas deverá comunicá-lo de imediato ao Tribunal Superior Eleitoral (TSE), ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), órgão superior vinculado ao Conselho Nacional de Justiça (CNJ), ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal.

Art. 19. Esta Portaria entra em vigor na data da sua publicação.

Belém, 21 de outubro de 2021.

Documento assinado eletronicamente por **LUZIA NADJA GUIMARAES NASCIMENTO**, **Presidente**, em 25/10/2021, às 13:22, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pa.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1410245** e o código CRC **45053988**.