TRIBUNAL REGIONAL ELEITORAL DO ACRE

PORTARIA PRESIDÊNCIA Nº 156/2023 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 II da Portaria nº 162, de 10 de junho de 2021, do Conselho Nacional de Justiça, que constitui o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-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;

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 que visam garantir a disponibilidade e integridade dos ativos tecnológicos deste Tribunal;

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 0000986-71.2023.6.01.8000,

I

R E S O L V E :

Art. 1º Instituir o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Tribunal Regional Eleitoral do Acre, nos termos deste ato.

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 2º O Protocolo de Gerenciamento de Crises Cibernéticas é complementar ao Protocolo de Prevenção de Incidentes Cibernéticos e prevê as ações responsivas a serem colocadas em prática quando ficar evidente que um incidente de segurança cibernética não será mitigado rapidamente

e poderá durar dias, semanas ou meses.

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

I - Comitê Gestor de Tecnologia da Informação - CGTIC: trata-se de comitê deste Tribunal que tem por competência estabelecer estratégias, indicadores e metas institucionais, aprovar planejamentos e orientar as iniciativas e investimentos tecnológicos dentro dos temas específicos da área de tecnologia da 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;

V - 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 a tecnologia;

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

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;

XIX - Incidente grave: evento que tenha causado dano, colocado em risco ativos críticos de informação ou interrompido a execução de atividades críticas;

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

XI - 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 São serviços de tecnologia da informação considerados críticos ao funcionamento do Tribunal, para efeito deste protocolo, aqueles considerados como essenciais pelo Comitê Gestor de Tecnologia da Informação (CGTIC) e validados pelo Comitê Setorial (COSET).

CAPÍTULO II
DA IDENTIFICAÇÃO DE CRISE CIBERNÉTICA

Art. 5º 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. 6º O gerenciamento de crise se inicia quando:

I - restar caracterizado grave dano material ou de imagem;

II - for evidenciada a possibilidade que as ações de resposta ao incidente cibernético persistirão por longo período;

III - o incidente impactar gravemente os serviços de TI essenciais ao funcionamento do Tribunal, extrapolando os limites determinados nas diretrizes do Plano de Continuidade dos Serviços Essenciais de TI (PCSTI) do TRE-AC (Portaria Presidência n. 76/2019);

IV - o incidente atrai grande atenção da mídia e da população em geral;

V - ocorrer vazamento de dados pessoais a partir de sistemas computacionais do TRE-AC.

CAPÍTULO III
DA COMPOSIÇÃO DO COMITÊ DE CRISES CIBERNÉTICAS

Art. 7º Fica instituído o Comitê de Crises Cibernéticas, para cumprimento das competências definidas neste Protocolo de Gerenciamento de Crises, com a seguinte formação:

I - Presidente do Tribunal de Regional Eleitoral do Acre;

II - Corregedor(a) Regional Eleitoral do Acre;

III - Diretor(a)-Geral;

IV - Secretário(a) de Tecnologia da Informação;

V - Secretário(a) Judiciário;

VI - Secretário(a) de Administração, Orçamento e Finanças;

VII - Coordenador(a) de Gestão de Pessoas;

VIII - Coordenador(a) da Comissão de Segurança da Informação (CSI);

IX - Membros do Comitê Gestor de Tecnologia da Informação (CGTIC);

X - Presidente da Comissão de Segurança da Institucional;

XI - Encarregado(a) de Tratamento de Dados no âmbito do TRE/AC;

XII - Assessor(a) de Comunicação do Tribunal.

Parágrafo único. O Comitê de Crises Cibernéticas será presidido pelo Presidente do Tribunal Regional Eleitoral do Acre e, na sua impossibilidade, será sucedido na ordem dos incisos deste artigo.

CAPÍTULO IV
DURANTE A CRISE

Art. 8º Caberá a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), identificando que o incidente de segurança constitui uma crise cibernética,

comunicar o fato ao Secretário de Tecnologia da Informação que acionará, por sua vez, o Comitê de Crises Cibernéticas que deverá se reunir imediatamente.

§ 1º Fica definida como sala de situação, local a partir do qual serão geridas as crises, a Sala de Reuniões da Diretoria-Geral, localizada no 3º andar da Secretaria do Tribunal ou outra que o Comitê de Crises Cibernéticas julgue mais adequada ou ainda, na impossibilidade de reunião presencial, virtualmente por meio de solução oficial de videoconferência adotada pelo TRE-AC para deliberar sobre o incidente que constitui a crise cibernética.

§ 2º Caso seja confirmada a crise cibernética, o Comitê de Crises Cibernéticas entrará em estado de convocação permanente, podendo se reunir a qualquer horário para discutir, deliberar e agir no tratamento da crise em curso.

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

§ 4º O Comitê de Crises Cibernéticas deve ter acesso ágil a meios que permitam fazer declarações públicas à imprensa.

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

§ 6º Os planos de contingências existentes, caso aplicáveis, devem ser efetivados imediatamente após a declaração da crise cibernética, visando à continuidade dos serviços prestados.

§ 7º A sala de situação deve dispor dos meios necessários (ex. sistemas de áudio, vídeo, chamadas telefônicas) e estar próxima a um local onde se possa fazer declarações públicas à imprensa.

Art. 9º Para eficácia do trabalho do Comitê de Crises Cibernéticas, é necessário que os esforços visem:

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 uma 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;

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 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;

XIV – elaborar plano de retorno à normalidade.

Art. 10 As etapas e procedimentos de resposta são diferentes a depender do tipo de crise e são necessárias reuniões regulares para avaliar o progresso até que seja possível retornar à condição de normalidade.

Art. 11 A Presidência do TRE-AC encaminhará comunicado da ocorrência do incidente grave quando constatada uma crise cibernética:

I - ao Tribunal Superior Eleitoral;

II - ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), órgão superior vinculado ao Conselho Nacional de Justiça;

III - ao Ministério Público Federal (MPF) e à Ordem dos Advogados do Brasil, Seccional Acre (OAB/AC), quando o incidente envolver a prestação jurisdicional.

Art. 12 Cabe ao encarregado(a) de tratamento de dados pessoais comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular de dados pessoais, ocorrência de incidente grave, envolvendo dados pessoais, que possa acarretar risco ou dano relevante aos titulares.

Art. 13 Cabe ao Secretário de Tecnologia da Informação:

I - identificar e manter documentação técnica atualizada dos ativos de informação que suportam os serviços essenciais;

II - avaliar e tratar os riscos de TI aos quais as atividades estratégicas estão expostas e que possam impactar diretamente na continuidade do negócio, de acordo com o processo de gestão de riscos de segurança da informação;

III - elaborar um plano de gestão de incidentes cibernéticos para os ativos críticos o qual deve possuir, no mínimo, as categorias de incidentes a que os ativos críticos estão sujeitos; a indicação do procedimento de resposta específico a ser aplicado em caso de ocorrência do incidente; e a severidade do incidente;

IV - elaborar e testar planos de contingência de TI para os serviços essenciais, sem prejuízo das ações decorrentes da norma complementar que estabelece as diretrizes para a gestão da continuidade de TI do TRE-AC.

Art. 14 Cabe ao Coordenador de Infraestrutura, que é também o Agente Responsável pela ETIR, comunicar a ocorrência de incidentes de segurança ao Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil – Cert.br.

CAPÍTULO V
FASE DE APRENDIZADO E REVISÃO (PÓS-CRISE)

Art. 15 Quando as operações retornarem à normalidade, o Comitê de Crises Cibernéticas deverá realizar a análise criteriosa das ações tomadas, observando as que foram bem-sucedidas e as que ocorreram de forma inadequada.

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 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;

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 e para a melhoria do processo de preparação para crises cibernéticas.

Art. 18 Após elaborado o relatório final a que se refere o caput do art. 16, deverá ser elaborado um plano de ação para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados.

Art. 19 As ações de resposta e recuperação da crise cibernética devem observar, ainda, no que couber, o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ), constante do Anexo II da Portaria n. 162, de 2021, do CNJ.

Art. 20 O protocolo estabelecido nesta portaria será revisto anualmente ou, quando necessário, em menor prazo.

Art. 21 Esta Portaria entra em vigor nesta data.

Desembargador **FRANCISCO DJALMA**

Presidente

Rio Branco, 18 de julho de 2023.

Documento assinado eletronicamente por **FRANCISCO DJALMA DA SILVA**, **Presidente**, em 21/07/2023, às 07:35, 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 **0599523** e o código CRC **1375DBEF**.