STM SUPERIOR TRIBUNAL MILITAR
DIDOC/COGES/LEGIS
Publicado no BJM nº 17,
de 03/05/2024

006732/23-00.039

PODER JUDICIÁRIO
SUPERIOR TRIBUNAL MILITAR

ATO NORMATIVO Nº 749

Institui o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito da Justiça Militar da União (JMU).

O MINISTRO-PRESIDENTE DO SUPERIOR TRIBUNAL MILITAR, no uso das atribuições que lhe são conferidas pelo art. 6°, inciso XXV, do Regimento Interno e,

CONSIDERANDO que é imprescindível garantir a segurança cibernética do ecossistema digital da Justiça Militar da União (JMU);

CONSIDERANDO a Resolução nº 396, do Conselho Nacional de Justiça (CNJ), de 7 de junho de 2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Resolução nº 370, do Conselho Nacional de Justiça (CNJ), de 28 de janeiro de 2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO o anexo II da Portaria nº 162, do Conselho Nacional de Justiça, de 10 de junho de 2021, que constitui o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ);

CONSIDERANDO a Norma ABNT NBR ISO/IEC 27001:2022, 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 a Política de Segurança Cibernética da JMU;

CONSIDERANDO o Relatório de Auditoria nº 8/2022 (SEI nº 2856351);

CONSIDERANDO o Plano de Ação elaborado pela Diretoria de Tecnologia da Informação (SEI nº 025093/22-00.047);

CONSIDERANDO que os ataques cibernéticos têm se tornado cada vez mais avançados e com alto potencial de prejuízo, que os impactos financeiros, operacionais e de reputação podem ser imediatos e significativos;

CONSIDERANDO que é fundamental aprimorar a capacidade do Poder Judiciário de coordenar pessoas, desenvolver recursos e aperfeiçoar processos, a fim de minimizar danos e agilizar o restabelecimento da condição de normalidade em caso de ocorrência de ataques cibernéticos de grande impacto,

R E S O L V E:

Art. 1º Este Ato Normativo institui o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ) no âmbito da Justiça Militar da União (JMU).

CAPÍTULO I
DAS 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 Ato Normativo, são estabelecidas as seguintes definições:

I - segurança cibernética: ações voltadas para a segurança de operações, com o objetivo de garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis;

II - segurança da informação: ações que objetivem viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

III - TIC: é uma sigla para Tecnologia da Informação e Comunicação, que faz referência ao conjunto de processos, *hardwares*, *softwares*, sistemas e funções de telecomunicações que proporcionem a automação e a sustentação de comunicação e processos das organizações;

IV - CGovTIC: trata-se do Comitê de Governança da Tecnologia da Informação e Comunicação para a JMU, 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 e segurança cibernética;

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

VI - crise cibernética: crise que ocorra em decorrência de incidentes em dispositivos, serviços e redes de computadores, que causem dano material ou de imagem, atraiam a atenção do público e da mídia e fujam ao controle direto da organização;

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

VIII - incidente cibernético: ocorrência que possa comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema, ou que possa revelar tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação de norma, política de segurança, procedimento de segurança ou política de uso;

IX - incidente grave: evento que cause dano, coloque em risco ativos críticos de informação ou interrompa a execução de atividades críticas; e

X - 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 à tecnologia.

Art. 4º São serviços de Tecnologia da Informação e Comunicação considerados críticos ao funcionamento da JMU, para efeito deste protocolo, os serviços essenciais assim definidos no Plano de Continuidade de Serviços de TIC.

CAPÍTULO II
DA IDENTIFICAÇÃO DE CRISE CIBERNÉTICA

Art. 5º O gerenciamento de incidentes refere-se às atividades que devem ser executadas na ocorrência de evento adverso de segurança cibernética para avaliar o problema e determinar a resposta

inicial.

Art. 6º O gerenciamento de crise será iniciado quando:

I - ficar caracterizado grave dano material ou de imagem;

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

III - houver grave impacto aos serviços de TIC, essenciais ao funcionamento do Tribunal, que extrapole os limites determinados nas diretrizes do Plano de Continuidade de Serviços de TIC da JMU;

IV - atrair grande atenção da mídia e da população em geral; e

V - ocorrer vazamento de quantidade significativa de dados pessoais.

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 representantes das seguintes áreas de atuação:

I - Presidência, responsável pela coordenação;

II - Corregedoria;

III - Jurídica;

IV - Comunicação Institucional;

V - Tecnologia da Informação e Comunicação;

VI - Privacidade de Dados e Informações;

VII - Segurança Cibernética;

VIII - Unidades administrativas de apoio à contratação; e

IX - Agente Responsável pela Equipe de Resposta a Incidentes de Segurança Cibernética.

§ 1º A nomeação dos integrantes do Comitê de Crises Cibernéticas ocorrerá a partir da publicação de Portaria específica.

§ 2º Na eventual ausência do titular, a unidade será representada pelo seu substituto legal.

Art. 8º O Comitê de Crises Cibernéticas tem como atribuições:

I - observar o Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário;

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

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

IV - avaliar plano de contingência de possíveis cenários de crise que tenha por objetivo manter os serviços prestados pelo Superior Tribunal Militar (STM);

V - avaliar o Plano de Resposta a Incidentes Cibernéticos da JMU;

VI - garantir a realização de simulações e de testes para validação dos planos de contingência e de resposta a incidentes cibernéticos;

VII - reunir imediatamente em sala de situação na ocorrência de crise cibernética;

VIII - garantir a efetiva comunicação e a atuação colaborativa entre as unidades durante a crise cibernética;

IX - garantir a documentação das lições aprendidas relacionadas aos eventos de crise; e

X - aprovar relatório final de eventos de crise.

CAPÍTULO IV
DO PERÍODO DE CRISE

Art. 9º Caberá à Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) comunicar ao Diretor de Tecnologia da Informação o incidente de segurança que constitui crise cibernética, após identificá-lo e classificá-lo.

§ 1º O incidente de segurança será comunicado ao Diretor-Geral da Secretaria do STM, que avisará imediatamente o Presidente do STM.

§ 2º O Presidente do STM decidirá sobre a necessidade de convocar o Comitê de Crises Cibernéticas.

§ 3º Em caso de convocação do Comitê de Crises Cibernéticas, será realizada imediatamente reunião na sala de situação, local a partir do qual serão geridas as crises.

§ 4º A sala de situação deverá dispor dos meios necessários (ex. sistemas de áudio, vídeo, chamadas telefônicas, *notebooks*) e estar próxima a um local onde seja possível fazer declarações públicas à imprensa.

§ 5º O local da sala de situação será definido na Portaria em que forem nomeados os integrantes do Comitê de Crises Cibernéticas.

§ 6º O membro impedido de reunir-se presencialmente, mediante justificativa formal ao Coordenador do Comitê de Crises Cibernéticas, poderá optar pelo formato virtual, utilizando solução oficial de videoconferência adotada pelo STM, para deliberar sobre o incidente que constitui a crise cibernética.

§ 7º Caso seja confirmada a crise cibernética, o Comitê de Crises Cibernéticas entrará em estado de convocação permanente e poderá reunir-se em qualquer horário para discutir, deliberar e agir no tratamento da crise em curso.

§ 8º O acesso às reuniões deverá ser restrito aos membros do Comitê e a atores eventualmente convidados.

§ 9º O Comitê de Crises Cibernéticas:

I - deverá ter acesso ágil a meios que permitam fazer declarações públicas à imprensa;

II - deverá contar com equipe dedicada à execução de atividades administrativas necessárias durante o período de crise; e

III - avaliará as ações de erradicação e planos de recuperação propostos pela ETIR.

§ 10 Os planos de contingências existentes, caso aplicáveis, deverão ser efetivados imediatamente após a declaração da crise cibernética, a fim de dar continuidade aos serviços prestados.

Art. 10. Para eficácia do trabalho do Comitê de Crise, 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 a desinformação 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 utilização 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 cibernética;

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

XI – avaliar a necessidade de recursos adicionais extraordinários para apoiar todos os integrantes envolvidos; e

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

Art. 11. As etapas e os procedimentos de resposta serão diferentes, a depender do tipo de crise, e serão necessárias reuniões regulares para avaliar o progresso até que seja possível retornar à condição de normalidade.

Art. 12. O Comitê de Crises Cibernéticas realizará as comunicações com atores internos e externos à JMU, conforme Plano de Comunicação de Crises Cibernéticas (PCCC).

Art. 13. Caberá à Diretoria de Tecnologia da Informação (DITIN):

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

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

III - elaborar um plano de resposta a incidentes cibernéticos para os ativos críticos, o qual deverá possuir, no mínimo, a indicação do procedimento de resposta específico a ser aplicado em caso de ocorrência do incidente; e

IV - elaborar e testar planos de contingência de TIC para os serviços essenciais, sem prejuízo das ações decorrentes da norma complementar que estabeleça as diretrizes para a gestão da continuidade de TIC da JMU.

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

Art. 14. Quando as operações retornarem à normalidade, o Comitê de Crises Cibernéticas deverá realizar a análise criteriosa das ações tomadas, com a identificação das que foram bem-sucedidas e das que ocorreram de forma inadequada.

Art. 15. Para a identificação das lições aprendidas e a elaboração de relatório final, deverão ser objeto de avaliação:

I – a identificação e a análise da causa do incidente;

II – a linha do tempo das ações realizadas;

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

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

V – o escalonamento da crise;

VI – a investigação e a preservação de evidências;

VII – a efetividade das ações de contenção;

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

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

Art. 16. As lições aprendidas deverão ser utilizadas para a elaboração ou revisão dos procedimentos específicos de resposta e para a melhoria na Gestão de Incidentes.

Art. 17. Deverá ser elaborado relatório com a descrição, o detalhamento da crise e o plano de ação tomado, para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, reduzam-se os danos causados.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 18. O protocolo estabelecido neste Ato Normativo será revisto quando ocorrer:

I - alteração no Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCC-PJ), estabelecido pelo CNJ;

II - alteração de normativos internos relacionados ao tema; e

III - estabelecimento de novos procedimentos técnicos ou implantação de novas tecnologias que impactem o funcionamento do protocolo.

Art. 19. Os casos omissos serão resolvidos pelo Ministro-Presidente do STM.

Art. 20. Este Ato Normativo entra em vigor na data de sua publicação.

Ten Brig Ar **FRANCISCO JOSELI PARENTE CAMELO**
Ministro-Presidente

Documento assinado eletronicamente por **FRANCISCO JOSELI PARENTE CAMELO**, **MINISTRO-PRESIDENTE DO SUPERIOR TRIBUNAL MILITAR**, em 26/04/2024, às 18:48 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.stm.jus.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **3714543** e o código CRC **38ABD016**.