VIII – Fabiana Andrade Gomes e Silva e Adilson Medeiros da Silva, como titular e suplente, respectivamente."(NR)

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

Ministro**LUIZ FUX**

PORTARIA Nº290, DE 17 DE DEZEMBRO DE 2020.

Institui o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Poder Judiciário (PGCC/ PJ).

O **PRESIDENTE DO CONSELHO NACIONAL DE JUSTIÇA (CNJ)**, nos termos da Resolução CNJ nº 360/2020, e no uso de suas atribuições legais e regimentais,

CONSIDERANDO competir ao CNJ a atribuição de coordenar o planejamento e a gestão estratégica de Tecnologia da Informação e Comunicação (TIC) do Poder Judiciário;

CONSIDERANDO que é imprescindível garantir a segurança cibernética do ecossistema digital do Poder Judiciário Brasileiro;

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 os termos da Resolução CNJ nº 211/2015, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), e estabeleceu as diretrizes para sua governança, gestão e infraestrutura;

CONSIDERANDO a importância de se estabelecer objetivos, princípios e diretrizes de Segurança da Informação alinhados às recomendações constantes da norma NBR ISO/IEC 27001:2013, que trata da segurança da informação;

CONSIDERANDO a importância de se estabelecer objetivos, princípios e diretrizes de Gestão de Riscos de Segurança da Informação alinhados às recomendações constantes da norma NBR ISO/IEC 27005:2019, que trata da gestão de riscos segurança da informação;

CONSIDERANDO a necessidade de se garantir o cumprimento da Lei Federal nº 12.527/2011 (Lei de Acesso à Informação), bem como, no âmbito do Poder Judiciário, da Resolução CNJ nº 215/2015, normas que disciplinam o direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral;

CONSIDERANDO o que dispõe a Lei Federal nº 13.709/2018, com a redação dada pela Lei Federal nº 13.853/2019, sobre a proteção de dados pessoais, que altera a Lei nº 12.965/2014 (Marco Civil da Internet);

CONSIDERANDO o disposto na Resolução CNJ nº 176/2013, que institui o Sistema Nacional de Segurança do Poder Judiciário;

CONSIDERANDO o disposto na Portaria CNJ nº 242//2020, que instituiu o Comitê de Segurança Cibernética do Poder Judiciário;

CONSIDERANDO o disposto na Portaria nº 249/2020, que designou os integrantes do Comitê de Segurança Cibernética do Poder Judiciário (CSCPJ);

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 de Poder Judiciário de coordenar pessoas, desenvolver recursos e aperfeiçoar processos, visando a minimizar danos e a agilizar o restabelecimento da condição de normalidade em caso de ocorrência de ataques cibernéticos de grande impacto;

RESOLVE:

Art. 1º Determinar a todos os órgãos do Poder Judiciário brasileiro, à exceção do Supremo Tribunal Federal, a adoção do Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCC/PJ).

Parágrafo único.O Protocolo previsto no *caput* possui caráter subsidiário, orientativo, suplementar e não substitui o conjunto de políticas de segurança da informação, processos de tratamento a incidentes e respostas ou procedimentos vigentes nos órgãos do Poder Judiciário.

CAPÍTULO I – DO OBJETIVO

Art. 2º Estabelecer um protocolo para o gerenciamento adequado de crises com o objetivo de contribuir para a resiliência corporativa por meio de uma resposta, a mais rápida e eficiente possível, a incidentes em que os ativos de informação do Poder Judiciário tenham a sua integridade, confidencialidade ou disponibilidade comprometidos em larga escala ou por longo período.

CAPÍTULO II – DO ESCOPO

Art. 3º O Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário 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.

CAPÍTULO III – DAS DEFINIÇÕES

Art. 4º Para os efeitos deste normativo, são estabelecidos os seguintes conceitos e definições:

I – Alta Administração: unidades organizacionais com poderes deliberativos ou normativos no âmbito da organização;

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

III – 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;

IV – Atividades críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão, de maneira que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;

V – 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 que eles geram, e que apresentam implicações que afetam uma proporção considerável da organização, bem como de seus constituintes;

VI – Crise cibernética: crise que ocorre em decorrência de incidente em dispositivos, serviços e redes de computadores. É decorrente de incidentes que causam dano material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização;

VII – Continuidade de negócios: capacidade estratégica e tática do órgão de se planejar e de responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

VIII – Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

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

X – Evento: qualquer ocorrência observável em um sistema ou rede de uma organização;

XI – Estratégia de continuidade de negócios: abordagem do órgão que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou com outro incidente maior;

XII – Gestão de riscos de segurança da informação: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e para equilibrá-los com os custos operacionais e financeiros envolvidos;

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

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

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

XVI – Incidente de Segurança da Informação: evento que viola ou representa uma ameaça iminente de violação de uma política de segurança, de uma política de uso aceitável ou de uma prática de segurança padrão;

XVII – Plano de gerenciamento de incidentes:plano de ação claramente definido e documentado, para ser usado quando ocorrer incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

XVIII – Procedimento: conjunto de ações sequenciadas e ordenadas para o atingimento de um determinado fim; e

XIX – Resiliência: poder de recuperação ou capacidade de determinada organização resistir aos efeitos de um incidente.

CAPÍTULO IV – DA IDENTIFICAÇÃO DE CRISE CIBERNÉTICA

Art. 5º O gerenciamento de incidentes se refere às atividades que devem ser executadas na ocorrência de um 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 – ficar caracterizado grave dano material ou de imagem;

II –restar evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses;

III – o incidente impactar a atividade finalística ou o serviço crítico mantido pela organização; ou

IV – atrair grande atenção da mídia e da população em geral.

CAPÍTULO V – DA FASE PREPARATÓRIA (PRÉ-CRISE)

Art. 7º Para melhor lidar com uma crise cibernética, é necessária prévia e adequada preparação, sendo fundamental que os órgãos do Poder Judiciário estabeleçam um Programa de Gestão da Continuidade de Negócios que contemple as seguintes atividades:

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

II – definir as atividades críticas 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 –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;

VI – priorizar o monitoramento, acompanhamento e tratamento dos riscos de maior criticidade. Tais atividades 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; e

VII – realizar simulações e testes para validação dos planos e procedimentos.

Art. 8º Deve ser definida a sala de situação e criado um Comitê de Crises Cibernéticas formado por representante da Alta Administração e por representantes executivos, suportados pela Equipe de Resposta a Incidentes de Segurança Cibernética e por especialistas das áreas:

I – Jurídica;

II – Comunicação;

III – Tecnologia da Informação;

IV – Privacidade de Dados Pessoais;

V – Segurança da Informação;

VI – Unidades administrativas de apoio à contratação; e

VII – Segurança Institucional.

Art. 9º O Plano de Gestão de Incidentes Cibernéticos 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.

Parágrafo único.O ANEXO I contém um exemplo básico de estruturação de Plano de Gestão de Incidentes Cibernéticos.

CAPÍTULO VI – DURANTE A CRISE

Art. 10. A comunicação entre todas as áreas envolvidas em uma crise é fator crítico para uma organização responder a uma crise cibernética de longa duração ou de grande impacto.

Art. 11. Assim que a Equipe de Tratamento e Resposta a Incidentes Cibernéticos identificar que um incidente constitui uma crise cibernética, deverá ser reunido imediatamente o Comitê de Crise na sala de situação previamente definida.

Parágrafo único. Os planos de contingência existentes, caso aplicáveis, devem ser efetivados imediatamente, visando à continuidade dos serviços prestados.

Art. 12. A chefia do Comitê de Crise deve ficar a cargo de profissional com autoridade e autonomia para tomar decisões sobre conteúdo de comunicados e textos a serem divulgados, bem como, delegar atribuições, estabelecer metas e prazos de ações.

Art. 13. A sala de situação é o local a partir do qual são geridas as situações de crise, devendo 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 e com o acesso restrito ao Comitê de Crise e a outros atores eventualmente convidados a participar de reuniões.

Parágrafo único. A sala de situação deve ser um ambiente que permita ao Comitê deliberar com tranquilidade e que possua uma equipe dedicada à execução de atividades administrativas para o período da crise.

Art. 14. Para eficácia do trabalho do Comitê de Crise, é necessário:

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 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 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 retorno à normalidade.

Art. 15. 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. 16. Todos os incidentes graves deverão ser comunicados ao órgão superior vinculado e ao Conselho Nacional de Justiça.

CAPÍTULO VII – FASE DE APREDIZADO E REVISÃO (PÓS-CRISE)

Art. 17. 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. 18. 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. 19. As lições aprendidas devem ser utilizadas para a elaboração ou revisão dos procedimentos específicos de resposta (*playbooks*) e a melhoria do processo de preparação para crises cibernéticas.

Art. 20. Deve ser elaborado relatório contendo a descrição e 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.

CAPÍTULO VIII – DISPOSIÇÕES FINAIS

Art. 21.Nos termos daPortaria CNJ nº 242/2020, que instituiu o Comitê de Segurança Cibernética do Poder Judiciário, e da Resolução CNJ nº 360/2020, que instituiu o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Poder Judiciário (PGCC/PJ), o protocolo definido neste ato normativo será objeto de reavaliação por ocasião da edição da Estratégia da Segurança Cibernética e da Informação do Poder Judiciário,bem como remanescerá passível de atualização a qualquer tempo.

Art. 22.Os órgãos do Poder Judiciário deverão elaborar e formalizar plano de ação, com vistas à construção de seus Protocolos de Gerenciamento de Crises Cibernéticas (PGCC/PJ), no prazo máximo de sessenta dias e comunicar a sua aprovação ao CNJ.

Art. 23.Esta Portaria entra em vigor na data de sua publicação, revogando-se as disposições em sentido contrário.

ANEXO I

Exemplo de Plano de Gestão de Incidentes Cibernéticos

Indicação do incidente cibernético	Descrição	Procedimento	Severidade
Campanha de *phishing*	O órgão é alvo de uma campanha de *phishing*	Identificação do documento de procedimento de resposta específico	Média
Degradação de serviços	Degradação ou interrupção de serviços ou sistemas por ataque de negação de serviço (DoS)	Identificação do documento de procedimento de resposta específico	Alta
Comprometimento de credenciais	Comprometimento de credenciais com acesso a informações sensíveis	Identificação do documento de procedimento de resposta específico	Alta
Impossibilidade de acesso a informação	Importantes informações organizacionais inacessíveis por encriptação (Ransomware)	Identificação do documento de procedimento de resposta específico	Crítica
Vazamento de informação e dados pessoais	Informações críticas encontradas fora da organização	Identificação do documento de procedimento de resposta específico	Crítica

PORTARIA Nº 291, DE 17 DE DEZEMBRO DE 2020.

Institui o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário.

O **PRESIDENTE DO CONSELHO NACIONAL DE JUSTIÇA (CNJ)**, no uso de suas atribuições legais e regimentais,e nos termos da Resolução CNJ nº 362/2020,

CONSIDERANDO o disposto nos incisos X e XII do art. 5º da Constituição da República, que instituem os direitos à privacidade;

CONSIDERANDO a Lei nº13.709/2018 – Lei Geral de Proteção de Dados;a Lei nº12.965/2014 – Marco Civil da Internet; o Decreto nº8.771/2016, e a Lei nº12.527/2011 – Lei de Acesso à Informação; bem como as Resoluções CNJ nº 121/2010 e nº 215/2015 e a Recomendação do CNJ nº 73/2020;

CONSIDERANDO a Portaria CNJ nº 242/2020, que institui o Comitê de Segurança Cibernética do Poder Judiciário e dispõe sobre a normatização para criação do Centro de Tratamento de Incidentes de Segurança Cibernética (CTISC) do CNJ, que funcionará como canal oficial para orquestração e divulgação de ações preventivas e corretivas, em caso de ameaças ou de ataques cibernéticos;

CONSIDERANDO a Instrução Normativa GSI nº 1/2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal;

CONSIDERANDO a Instrução Normativa GSI nº 2/2020, que altera a Instrução Normativa GSI nº 1/2020, a qual dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal;