Poder Judiciário

Conselho Nacional de Justiça

ANEXO II – Protocolo – Gerenciamento de crises cibernéticas do Poder Judiciário

Protocolo

Gerenciamento de Crises Cibernéticas do Poder Judiciário

Material de referência com as principais diretrizes para implantação do protocolo de gerenciamento de Crises Cibernéticas do Poder Judiciário

Sumário

Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ)

1. Escopo

1.1. 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.

2. Identificação de Crise Cibernética

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

2.2. O gerenciamento de crise se inicia quando:

a) ficar caracterizado grave dano material ou de imagem;
b) restar evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses;
c) o incidente impactar a atividade finalística ou o serviço crítico mantido pela organização; ou
d) o incidente atrair grande atenção da mídia e da população em geral.

3. Fases do Gerenciamento de Crises

3.1 O Gerenciamento de Crises pode ser dividido em 3 (três) fases:

a) Planejamento (pré-crise);
b) Execução (durante a crise);
c) Melhoria Contínua (pós-crise).

4. Planejamento da Crise (pré-crise)

4.1 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 Serviços que contemple as seguintes atividades:

a) observar o Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário;
b) definir as atividades críticas que são fundamentais para a atividade finalística do órgão;
c) 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;
d) avaliar continuamente os riscos a que as atividades críticas estão expostas e que possam impactar diretamente na continuidade do negócio;
e) 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;
f) 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 manter os serviços prestados pela organização; e
g) realizar simulações e testes para validação dos planos e procedimentos.

4.2 Deve-se definir a sala de situação e criar um Comitê de Crises Cibernéticas, composto por representantes da alta administração e por representantes executivos, com suporte da Equipe de Resposta a Incidentes de Segurança Cibernética (ETIR) e de especialistas:

a) da área Jurídica;
b) da área de Comunicação Institucional;
c) da área de Tecnologia da Informação e Comunicação;
d) da área de Privacidade de Dados Pessoais;
e) da área de Segurança da Informação;

f) das unidades administrativas de apoio à contratação; e

g) da área de Segurança Institucional.

4.3 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.

5. Execução (durante a crise)

5.1 A comunicação entre as áreas envolvidas é fator fundamental para uma organização reagir a uma crise cibernética de longa duração ou de grande impacto.

5.2 Assim que a ETIR identificar que um incidente constitui uma crise cibernética, o Comitê de Crise deverá se reunir imediatamente na sala de situação previamente definida.

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

5.4 A chefia do Comitê de Crise deve ficar a cargo de profissional, indicado pelo Presidente do respectivo órgão do Poder Judiciário, com autoridade e autonomia para tomar decisões sobre conteúdo de comunicação a serem divulgados, bem como delegar atribuições, estabelecer metas e prazos de ações.

5.5 A sala de situação é o local a partir do qual serão 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 acesso restrito ao Comitê de Crise e a outros entes eventualmente convidados a participar das reuniões.

5.6 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.

5.7 Para eficácia do trabalho, é necessário o Comitê de Crise:

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

b) levantar todas as informações relevantes, verificando fatos e descartando boatos;
c) levantar soluções alternativas para a crise, avaliando sua viabilidade e consequências;
d) avaliar a necessidade de suspender serviços e/ou sistemas informatizados;
e) centralizar a comunicação na figura de um porta-voz para evitar informações equivocadas ou imprecisas;
f) 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;
g) definir estratégias de comunicação com a imprensa e/ou redes sociais e estabelecer qual a mídia mais adequada para se utilizar em cada caso;
h) aplicar o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário;
i) solicitar a colaboração de especialistas ou de centros de resposta a incidentes de segurança;
j) apoiar equipes de resposta e de recuperação com gerentes de crise experientes;
k) avaliar a necessidade de recursos adicionais extraordinários a fim de apoiar as equipes de resposta;
l) orientar sobre as prioridades e estratégias da organização para recuperação rápida e eficaz;
m) definir os procedimentos de compartilhamento de informações relevantes para a proteção de outras organizações com base nas informações colhidas sobre o incidente; e
n) elaborar plano de retorno à normalidade.

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

5.9 Todos os incidentes graves deverão ser comunicados ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), órgão superior vinculado ao Conselho Nacional de Justiça.

6. Melhoria contínua (lições aprendidas no pós-crise)

6.1 Após o retorno das operações 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.

6.2 Para a identificação das lições aprendidas e a elaboração de relatório final, devem ser objeto de avaliação:

a) a identificação e análise da causa-raiz do incidente;
b) a linha do tempo das ações realizadas;
c) a escala do impacto nos dados, sistemas e operações de negócios importantes durante a crise;
d) os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas;
e) o escalonamento da crise;
f) a investigação e preservação de evidências;
g) a efetividade das ações de contenção;
h) a coordenação da crise, liderança das equipes e gerenciamento de informações; e
i) a tomada de decisão e as estratégias de recuperação.

6.3 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.

6.4 Deve ser elaborado Relatório de Comunicação de Incidente de Segurança em Redes Computacionais, que contenha 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.

7. Exemplo de Plano de Gestão de Incidentes Cibernéticos

Item	Indicação do incidente cibernético	Descrição	Procedimento	Severidade
1	Campanha de *phishing*	O órgão é alvo de uma campanha de *phishing*.	Identificação do documento de procedimento de resposta específico.	Média
2	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
3	Comprometimento de credenciais	Comprometimento de credenciais com acesso a informações sensíveis.	Identificação do documento de procedimento de resposta específico.	Alta
4	Impossibilidade de acesso à informação	Importantes informações organizacionais inacessíveis por encriptação (*ransomware*).	Identificação do documento de procedimento de resposta específico.	Crítica
5	Vazamento de informação e dados pessoais	Informações críticas encontradas fora da organização.	Identificação do documento de procedimento de resposta específico.	Crítica