Poder Judiciário

Conselho Nacional de Justiça

ANEXO I – Protocolo – Prevenção de incidentes cibernéticos do Poder Judiciário

Protocolo

Prevenção de Incidentes Cibernéticos do Poder Judiciário

Material de referência com as principais diretrizes necessárias para implantação do protocolo de prevenção de incidentes cibernéticos do Poder Judiciário

Sumário

Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ)

1. Escopo

1.1 O Protocolo de Prevenção a Incidentes Cibernéticos contemplará um conjunto de diretrizes para a prevenção a incidentes cibernéticos em seu mais alto nível.

1.2 As diretrizes serão divididas em funções que expressem a gestão do risco organizacional e que permitam as decisões adequadas para o enfrentamento de ameaças e a melhor gestão de práticas e de metodologias existentes.

1.3 As diretrizes poderão ser adaptadas, incrementadas ou ajustadas considerando-se a realidade de cada órgão do Poder Judiciário.

2. Funções básicas

2.1 São funções básicas do Protocolo de Prevenção a Incidentes Cibernéticos: identificar, proteger, detectar, responder e recuperar, nos seguintes termos.

2.1.1 **identificar:** entendimento organizacional para gerenciar o risco de ataques cibernéticos a sistemas, pessoas, ativos, dados e recursos. Permite ao órgão avaliar os recursos que suportam funções críticas e os riscos relacionados. São medidas de concentração e priorização dos esforços na gestão de ativos, ambiente de negócios, governança, avaliação de riscos e estratégia de gestão de riscos.

2.1.2 **proteger:** desenvolvimento e implementação de salvaguardas que assegurem a proteção de dados, inclusive pessoais, de ativos de informação; e a prestação de serviços críticos. Possibilita aos órgãos suportar e conter impactos ocasionados por incidentes cibernéticos. Nessa função, estão incluídas as seguintes medidas, sem prejuízo de outras eventualmente adotadas: gerenciamento de identidade e controle de acesso, conscientização e treinamento, segurança de dados, processos e procedimentos de proteção da informação, medidas de atualização, manutenção e tecnologias de proteção.

2.1.3 **detectar:** desenvolvimento e implementação de atividades adequadas à descoberta oportuna de eventos ou à detecção de incidentes de segurança

cibernética. Estão contempladas ações de monitoramento contínuo de segurança, processos de detecção de anomalias e eventos.

2.1.4 **responder:** desenvolvimento e implementação de atividades apropriadas à adoção de medidas em incidentes cibernéticos detectados. Nessa categoria, são incluídos os planos de resposta, de comunicações, de análise, de mitigação e de melhorias.

2.1.5 **recuperar:** desenvolvimento, implementação e manutenção dos planos de resiliência e de restauração de quaisquer capacidades ou serviços que foram prejudicados em razão de incidentes de segurança cibernética.

3. Princípios críticos

3.1 O protocolo de prevenção a incidentes cibernéticos criado no âmbito de cada tribunal contemplará um conjunto de princípios críticos que assegurem a construção de sistema de segurança cibernética eficaz.

3.2 São princípios críticos que podem ser adaptados, incrementados ou ajustados, considerada a realidade de cada órgão do Poder Judiciário:

3.2.1 **base de conhecimento de defesa**: consiste no uso de informações e conhecimento de ataques reais que comprometeram sistemas. Informações conseguidas por meio de interação e de cooperação com outras equipes de tratamento a incidentes e respostas. Tem por propósito fornecer bases fundamentais ao aprendizado contínuo com apoio em eventos ocorridos. Apoia a construção de defesas eficazes e práticas.

3.2.2 **priorização:** foco prioritário na formação, na revisão de controles, nos processos e na disseminação da cultura de segurança cibernética. Contribui para a redução de riscos e para a proteção contra as ameaças mais sensíveis e que encontram viabilidade em sua célere implementação.

3.2.3 **instrumentos de medição e métricas:** definição e estabelecimento de métricas comuns que fornecem linguagem compartilhada e de compreensão abrangente para magistrados e magistradas, servidores e servidoras, colaboradores e colaboradoras, prestadores e prestadoras de serviços, especialistas em tecnologia da informação, auditores e demais atores do sistema de segurança. Permite a

medição da eficácia das medidas de segurança dentro da organização. Fornece insumos para que os ajustes necessários, quando identificados, possam ser implementados de forma célere.

3.2.4 **diagnóstico contínuo:** processo de trabalho que realiza continuamente medição para testar e validar a eficácia das medidas de segurança atuais e contribui para a definição de prioridades e para os próximos passos a serem tomados.

3.2.5 **formação e capacitação:** processos formais de educação continuada com a inclusão em planos de capacitação que contemplem a disseminação, a formação e a instrução para todos os atores envolvidos em atividades diretas ou indiretas que contribuam para a cultura de segurança cibernética dentro da organização. Tais instrumentos deverão ser revisados periodicamente.

3.2.6 **automação:** incentivo à busca de soluções automatizadas de segurança cibernética para que as organizações obtenham medições confiáveis, escaláveis e contínuas. Tal processo está correlacionado com os resultados almejados por meio dos instrumentos de controle e de métricas**.**

3.2.7 **resiliência:** poder de recuperação ou capacidade de a organização resistir aos efeitos de um incidente.

4. Gestão de Incidentes de Segurança da Informação

4.1 A gestão de incidentes de segurança da informação é realizada por meio de processo definido e constituída formalmente, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança.

5. Competência de atuação

5.1 Deverá ser formalmente instituída Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR), em todos os órgãos do Poder Judiciário, à exceção do STF.

5.2 A ETIR poderá solicitar apoio multidisciplinar que abranja as áreas: tecnologia da informação, segurança da informação, jurídica, pesquisas judiciárias, comunicação, controle interno, segurança institucional, entre outras, necessárias para responder aos incidentes de segurança de maneira adequada e tempestiva.

5.3 Caberá a cada órgão do Poder Judiciário avaliar o adequado posicionamento da ETIR em seu organograma institucional, considerando-se seu desenho organizacional e suas peculiaridades.

5.4 A ETIR terá autonomia compartilhada, ou seja, participará do resultado da decisão recomendando os procedimentos a serem executados ou as medidas de recuperação durante a identificação de uma ameaça e debaterá sobre as ações a serem tomadas, seus impactos e a repercussão, caso as recomendações não sejam seguidas.

6. Funcionamento da ETIR

6.1 O funcionamento da ETIR é regulado por documento formal de constituição, publicado no sítio eletrônico do respectivo órgão, devendo constar, no mínimo, os seguintes pontos:

a) definição da missão;
b) público-alvo;
c) modelo de implementação;
d) nível de autonomia;
e) designação de integrantes;
f) canal de comunicação de incidentes de segurança; e
g) serviços que serão prestados.

7. Boas Práticas de Segurança Cibernéticas

7.1 A segurança cibernética é um empreendimento coletivo.

7.2 Para melhor detectar, conter e eliminar ataques cibernéticos e minimizar eventuais impactos na operação, assegurando o funcionamento dos sistemas críticos do Poder Judiciário, sobretudo em ambiente de constante ameaça, é necessário que todos os seus órgãos possuam mecanismos de respostas e prevenção.

7.3 A prevenção a incidentes contempla funções de preparação, identificação, contenção, erradicação, recuperação e lições aprendidas.

7.4 As dimensões e práticas poderão ser adaptadas, incrementadas ou ajustadas conforme a realidade de cada órgão.

7.5 São assim definidas as dimensões e práticas da segurança cibernética:

7.5.1 **preparação:** processo que envolve as equipes de tratamento a incidentes e respostas. Trata-se de resposta metódica, contemplando ferramentas forenses de análise e custódia, identificação de cadeia de comando em situação de crise, processos de educação e de formação.

7.5.2 **identificação:** capacidade de identificar que um ataque cibernético está em andamento, por meio da percepção de sinais de anomalias ou de comportamentos inesperados. Trata-se da aptidão dos entes para diferenciar as irregularidades em redes de dados e identificar o mau funcionamento dos sistemas críticos, em razão de ataques cibernéticos em curso. Para essa atividade, podem ser elaboradas listas de verificação investigativas para apoiar o processo de diagnóstico, triagem e acionamento das equipes de resposta, permitindo a avaliação do impacto e a determinação dos próximos passos a serem tomados.

7.5.3 **contenção:** visa a garantir que o incidente não cause mais danos, por meio da adoção dos mecanismos de comunicação previstos no Protocolo de Gerenciamento de Crises. Nessa dimensão, a prioridade geral é isolar o que foi afetado, manter a produção e, acima de tudo, garantir que as ações não comprometam, ainda mais, a segurança ou as operações críticas. Tal atividade tende a ser complexa, devendo os utilitários isolar a fonte de um ataque e determinar o momento de aplicação de ferramenta forense passiva construída para remoção de malware das redes de produção ou para a limitação de transferências de dados desnecessárias**.**

7.5.4 **erradicação:** remoção da ameaça, garantindo que as operações essenciais sejam apoiadas, caso surjam desafios no processo de restauração. Os métodos possíveis para essa função podem variar desde patches ou reconstruções do sistema até redesenho completo da arquitetura, devendo, sempre que possível, preservar evidências que apoiarão o processo de investigação do crime cibernético.

7.5.5 **recuperação:** promulgação de plano de recuperação em fases para restauração de operações, com foco prioritário nos sistemas críticos ou na execução da operação em modo analógico até que haja confiança no desempenho do sistema. Nessa atividade, são necessárias verificações ambientais e de segurança

paralelas ao controle dos impactos de desempenho não intencionais da restauração.

7.5.6 **lições aprendidas:** atividade contínua que não só deve capturar os impactos imediatos de um incidente, mas também as melhorias em longo prazo da segurança cibernética do órgão. Tal função pode variar de um sistema de controle de processos melhor projetado até a evolução e preparação de centros de identificação e resposta a ataques cibernéticos do Poder Judiciário.