CONSELHO NACIONAL DE JUSTIÇA
PRESIDÊNCIA

PORTARIA Nº 292, DE 17 DE DEZEMBRO DE 2020.

Determina a adoção de Protocolo de Prevenção a Incidentes Cibernéticos no âmbito do Poder Judiciário (PPICiber/PJ).

O **PRESIDENTE DO CONSELHO NACIONAL DE JUSTIÇA (CNJ)**, uso de suas atribuições legais e regimentais, e nos termos da Resolução CNJ nº 361/2020,

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 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 de receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral;

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

Fonte: Diário da Justiça [do] Conselho Nacional de Justiça, Brasília, DF, n. 397, p. 21-24, 17 dez. 2020.

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 CNJ nº 249/2020, que designou os integrantes do Comitê de Segurança Cibernética do Poder Judiciário (CSCPJ);

RESOLVE:

Art. 1º Determinar a todos os órgãos do Poder Judiciário brasileiro, à exceção do Supremo Tribunal Federal, a adoção de Protocolo de Prevenção a Incidentes Cibernéticos (PPICiber/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 em cada um dos órgãos do Poder Judiciário.

CAPÍTULO I
DO ESCOPO

Art. 2º. O Protocolo de Prevenção a Incidentes Cibernéticos contemplará um conjunto de diretrizes para a prevenção a incidentes cibernéticos em seu mais alto nível.

§ 1º As diretrizes serão divididas em funções que expressem a gestão do risco organizacional e que permitam decisões adequadas para o enfrentamento de ameaças e a melhor gestão de práticas e de metodologias existentes.

§ 2º As diretrizes poderão ser adaptadas, incrementadas ou ajustadas considerando a realidade de cada órgão do Poder Judiciário.

Art. 3º São funções básicas do Protocolo de Prevenção a Incidentes Cibernéticos a de identificar, proteger, detectar, responder e recuperar, nos seguintes termos:

I – Identificar: consiste no entendimento organizacional para gerenciar o risco de ataques cibernéticos a sistemas, pessoas, ativos, dados e a 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 na estratégia de gestão de riscos.

II – Proteger: desenvolvimento e implementação de salvaguardas que assegurem a proteção de dados, inclusive pessoais, 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.

III – Detectar: corresponde ao desenvolvimento e à implementação de atividades adequadas à descoberta oportuna de eventos ou para a detecção de incidentes de segurança cibernética. Estão contempladas ações de monitoramento contínuo de segurança, processos de

Fonte: Diário da Justiça [do] Conselho Nacional de Justiça, Brasília, DF, n. 397, p. 21-24, 17 dez. 2020.

detecção de anomalias e eventos.

IV – 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.

V – 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.

Art. 4º 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.

§ 1º São princípios críticos:

I – 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.

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

III – Instrumentos de Medição e Métricas: definição e estabelecimento de métricas comuns que fornecem linguagem compartilhada e de compreensão abrangente para magistrados, servidores, colaboradores, prestadores 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.

IV – Diagnóstico contínuo: cuida do 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.

V – 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.

VI – 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.

VII – Resiliência: poder de recuperação ou capacidade de uma organização de resistir aos efeitos de um incidente.

§ 2º Os princípios podem ser adaptados, incrementados ou ajustados considerada a realidade de cada órgão do Poder Judiciário.

CAPÍTULO II
DA GESTÃO DE INCIDENTES DE SEGURANÇA

Art. 5º A gestão de incidentes de segurança cibernética é realizada por meio de processo definido e constituída formalmente, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança.

Art. 6º Deverão ser formalmente instituídas Equipes de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR).

§ 1º As ETIR poderão solicitar apoio multidisciplinar abrangendo as áreas de tecnologia da informação, jurídica, pesquisas judiciárias, comunicação, controle interno, segurança institucional, dentre outras necessárias para responder aos incidentes de segurança de maneira adequada e tempestiva.

§ 2º Caberá a cada órgão avaliar, considerada suas peculiaridades e desenho organizacional, o adequado posicionamento das ETIR em seu organograma institucional.

Art. 7º As ETIR têm 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 as ações a serem tomadas, seus impactos e a repercussão, caso as recomendações não sejam seguidas.

Art. 8º O funcionamento das ETIR é regulado por documento formal de constituição, publicado no sítio eletrônico do respectivo órgão, devendo constar, no mínimo, os seguintes pontos: definição da missão, público-alvo, modelo de implementação, nível de autonomia, designação de integrantes, canal de comunicação de incidentes de segurança e os serviços que serão prestados.

CAPÍTULO IV
DA SEGURANÇA CIBERNÉTICA E BOAS PRÁTICAS

Art. 9º Para melhor detectar, conter e eliminar ataques cibernéticos, bem como para minimizar eventuais impactos na operação, assegurando o funcionamento dos sistemas críticos do Poder Judiciário brasileiro, sobretudo em ambiente de constante ameaça, é necessário que todos os seus órgãos possuam mecanismos de respostas e prevenção.

Art. 10. A prevenção a incidentes contempla funções de preparação, identificação, contenção, erradicação, recuperação e lições aprendidas.

§ 1º As dimensões e práticas poderão ser adaptadas, incrementadas ou ajustadas em razão da realidade de cada órgão.

§ 2º A segurança cibernética é um empreendimento coletivo.

§ 3º São assim definidas as dimensões e práticas da segurança cibernética:

I – Preparação: processo que envolve as equipes de tratamento a incidentes e respostas. Cuida-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.

II – 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 times para diferenciar irregularidades em redes de dados e o mal funcionamento dos sistemas críticos, em razão de ataques cibernéticos em curso. Para essa atividade, listas de verificação investigativas podem ser elaboradas 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.

III – 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 infecções, 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, por essa razão, 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.

IV – Erradicação: consiste na 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.

V – Recuperação: promulgação de plano de recuperação em fases para restauração de operações, com o foco prioritário em sistemas críticos ou na execução da operação em modo analógico até que haja confiança no desempenho em nível de sistema. Nessa atividade, são necessárias verificações ambientais e de segurança paralelas ao controle dos impactos de desempenho não intencionais da restauração.

VI – Lições Aprendidas: o processo de lições aprendidas é uma 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.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 11. Nos termos da Portaria CNJ nº 242/2020, que instituiu o Comitê de Segurança Cibernética do Poder Judiciário, e da Resolução CNJ nº 361/2020, que determinou a adoção do Protocolo de Prevenção a Incidentes Cibernéticos no âmbito do Poder Judiciário (PPICiber/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. 12. Os órgãos deverão elaborar e formalizar plano de ação com vistas à construção do seu Protocolo de Prevenção a Incidentes Cibernéticos, PPICiber/Pj, no prazo máximo de sessenta dias e comunicar ao CNJ.

Art. 13. Esta Portaria em vigor na data de sua publicação, revogando-se as disposições em contrário.

Ministro LUIZ FUX

Fonte: Diário da Justiça [do] Conselho Nacional de Justiça, Brasília, DF, n. 397, p. 21-24, 17 dez. 2020.