PODER JUDICIÁRIO DA UNIÃO
TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO
GABINETE DA PRESIDÊNCIA
GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO

Institui o Protocolo de Prevenção de Incidentes Cibernéticos no âmbito do Tribunal Regional do Trabalho da 18ª Região.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO, no uso de suas atribuições legais e regimentais, tendo em vista o que consta dos Processos Administrativos nº 15452/2020 e nº 12772/2021;

CONSIDERANDO a Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Portaria CNJ nº 162/2021, que aprova Protocolos e Manuais criados pela ENSEC-PJ, em especial seu anexo I,

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Portaria institui o Protocolo de Prevenção de Incidentes Cibernéticos (PPINC), aplicável no âmbito do Tribunal Regional do Trabalho da 18ª Região.

Art. 2º Para os fins desta Portaria, consideram-se as definições constantes do anexo VIII (Glossário) da Portaria CNJ nº 162/2021.

CAPÍTULO II
DAS DIRETRIZES

Art. 3º Fica estabelecida a Estrutura Básica do PPINC, conforme modelo do Anexo I desta Portaria.

§ 1º A Estrutura Básica do PPINC agrupa as diretrizes de prevenção a incidentes, em seu mais alto nível, em funções básicas que expressam a gestão do risco organizacional e que permitem as decisões adequadas para o enfrentamento de ameaças e a melhor gestão de práticas e de metodologias.

§ 2º A unidade responsável pela gestão de segurança da informação manterá atualizada e publicada a estrutura básica do PPINC.

§ 3º Por deliberação do colegiado que atua como instância de apoio à governança de segurança da informação, as diretrizes referidas no § 1º deste artigo poderão ser adaptadas, incrementadas ou ajustadas.

Art. 4º São funções básicas do PPINC: identificar, proteger, detectar, responder e recuperar, nos seguintes termos:

I – **identificar**: entendimento organizacional para gerenciar o risco direto e/ou indireto 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;

II – **proteger**: desenvolvimento e implementação de salvaguardas que assegurem a proteção de dados, inclusive pessoais, e de ativos de informação, bem como a prestação de serviços críticos;

III – **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;

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.

CAPÍTULO III
DOS PRINCÍPIOS CRÍTICOS

Art. 5º Ao estabelecer, manter e aprimorar um sistema de segurança cibernética eficaz, os seguintes princípios críticos deverão ser observados:

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, na revisão de controles/acessos, 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;

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**: 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, capacitação e conscientização**: processos formais de educação continuada com a inclusão em planos de capacitação que contemplem a disseminação, a formação, a conscientização 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 a organização resistir aos efeitos de um incidente, bem como impedir a reincidência secundária do incidente identificado.

CAPÍTULO IV
DA GESTÃO DE INCIDENTES

Art. 6º 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.

Parágrafo único. O referido processo faz parte da gestão de incidentes de segurança da informação do órgão e deve implementar, no que couber, as atividades de tratamento e resposta a incidentes que envolvam dados pessoais.

CAPÍTULO V
DA COMPETÊNCIA DE ATUAÇÃO E FUNCIONAMENTO DA ETIR

Art.7º A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) é instituída e tem seu funcionamento regulado por Portaria específica, que observa as diretrizes indicadas nos itens 5 e 6 do anexo I à Portaria CNJ nº 162/2021.

CAPÍTULO VI
DAS BOAS PRÁTICAS DE SEGURANÇA CIBERNÉTICA

Art.8º A elaboração, revisão e execução dos processos de gerenciamento de incidentes de segurança cibernética no âmbito deste Regional, com seus respectivos mecanismos de resposta e prevenção, são essenciais à funcionalidade sistêmica do Poder Judiciário, e contemplarão as seguintes dimensões e práticas, que poderão ser adaptadas, incrementadas ou ajustadas conforme a realidade do Tribunal:

I – **preparação**: processo que envolve as equipes de tratamento a incidentes e respostas. Trata-se de resposta metódica, contemplando ferramentas forenses de análise e custódia, planejamento sobre como responder e notificar cada incidente de segurança, 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 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;

III – **contenção**: visa a garantir que o incidente não cause mais danos. 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 incluindo, dentre outros, a imediata comunicação prevista na Estratégia Nacional de Segurança Cibernética do Poder Judiciário

(ENSEC-PJ) e seus anexos, o isolamento da fonte do ataque, a aplicação de ferramentas forenses para remoção de malware das redes de produção, a limitação de transferências de dados desnecessárias e a adoção dos mecanismos de comunicação previstos no Protocolo de Gerenciamento de Crises Cibernéticas;

IV – **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;

V – **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;

VI – **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.

CAPÍTULO VII
DAS DISPOSIÇÕES FINAIS

Art. 9º Esta Portaria entra em vigor na data de sua publicação.

Publique-se no Diário Eletrônico da Justiça do Trabalho.

(assinado eletronicamente)
DANIEL VIANA JÚNIOR
Desembargador-Presidente
TRT da 18ª Região

Anexo I

Estrutura Básica do PPINC

Funções Básicas	Categorias*	Subcategorias*	Referências Informativas*
IDENTIFICAR	• Gestão de Ativos • ... • Gestão de Riscos de S.I. • ...	• Inventário e controle de ativos (*devices*) organizacionais • Inventário e controle de ativos de *software* • ...	CIS Controls v.8 - controles nº 01 e nº 02 NBR ISO/IEC 27002:2013 - Objetivo de Controle nº 8 ...
PROTEGER	• • ... •		
DETECTAR	• • ... •		
RESPONDER	• • ... •		
RECUPERAR	• • ... •		

* as informações nestas colunas são exemplificativas

Obs.:

- colunas com fundo cinza são opcionais, com uso sugerido para comunicação entre as áreas de gestão e técnicas;
- outras colunas poderão ser acrescentadas, a depender do que se pretende comunicar, por exemplo: percentual projetado e realizado de implementação de medidas, práticas e controles de segurança cibernética; percentual do risco de segurança cibernética residual identificado e consolidado por função básica ou por subcategoria etc.

Goiânia, 2 de junho de 2022.
[assinado eletronicamente]

DANIEL VIANA JÚNIOR

DESEMB. PRES. DE TRIBUNAL