ATO TRT13 SGP N.º 104, DE 15 DE AGOSTO DE 2022

Institui o Protocolo de Prevenção de Incidentes Cibernéticos (PPINC) no âmbito do Tribunal Regional do Trabalho da 13ª Região.

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA DÉCIMA TERCEIRA REGIÃO, no uso de suas atribuições legais e regimentais, nos termos do PROAD Nº 7443/2022,

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA DÉCIMA TERCEIRA REGIÃO, no uso de suas atribuições legais e regimentais,

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

CONSIDERANDO a Portaria CNJ nº 162/2021, que aprovou os protocolos e manuais criados pela ENSEC-PJ;

CONSIDERANDO as diretrizes da Política de Segurança da Informação e Comunicações da instituição;

CONSIDERANDO que a Segurança da Informação abrange a Segurança Cibernética;

CONSIDERANDO a necessidade de aprimoramento da instituição na coordenação de pessoas, desenvolvimento de recursos e aperfeiçoamento de processos, visando minimizar a ocorrência de ataques cibernéticos de grande impacto financeiro e operacional,

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Estabelecer o Protocolo de Prevenção de Incidentes Cibernéticos (PPINC) no âmbito do Tribunal Regional do Trabalho da 13ª Região, tendo como principais objetivos:

I - Estabelecer um conjunto de diretrizes de alto nível para a prevenção de incidentes cibernéticos;

II - Promover alinhamento às regulamentações, normas e melhores práticas relacionadas à Segurança Cibernética;

III - Promover ações que contribuam para a prevenção de incidentes cibernéticos e para a resiliência do ambiente tecnológico do Tribunal a ataques cibernéticos.

Art. 2º Para efeitos deste Ato, aplicam-se as definições da Política de Segurança da Informação e Comunicações, da Política de Proteção de Dados Pessoais e do Anexo VIII da Portaria CNJ nº 162/2021, além das seguintes:

I - Incidente cibernético: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

II - Segurança Cibernética: segmento da Segurança da Informação que visa proteger as informações armazenadas nos computadores e aparelhos de computação, e transmitidas através das redes de comunicação, incluindo a Internet.

Art. 3º As ações e medidas elencadas no presente protocolo são complementares às políticas, normas, procedimentos e processos institucionais relacionados à Segurança da Informação.

Art. 4º Esse protocolo integra o conjunto de protocolos de Segurança Cibernética instituídos pela Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

CAPÍTULO II

DAS FUNÇÕES DO PPINC

Art. 5º As diretrizes do PPINC são divididas em funções 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 existentes.

Art. 6º São funções básicas do presente protocolo, conforme definido na ENSEC-PJ: identificar, proteger, detectar, responder e recuperar.

Seção I

Da Função Identificar

Art. 7º A função “Identificar” consiste em atividades para identificar ativos tecnológicos críticos, levantar, analisar e avaliar os riscos aos quais o ambiente tecnológico está exposto, possibilitando a priorização e concentração de recursos humanos, tecnológicos e financeiros de acordo com a criticidade.

Art. 8º No âmbito da instituição, a função é contemplada pela seguinte atividade: Execução do Processo de Gestão de Riscos de Segurança da Informação, instituído por Ato da Presidência.

Seção II

Da Função Proteger

Art. 9º A função “Proteger” consiste no 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.

Art. 10. No âmbito da instituição, a função é contemplada pelas seguintes atividades:

I - Execução do Processo do Sistema de Gestão de Segurança da Informação, instituído por Ato da Presidência;

II - Execução do Processo de Gestão de Continuidade de TIC, instituído por Ato da Presidência;

III - Execução do Processo de Gestão de Vulnerabilidades de TIC, instituído por Ato da Presidência;

IV - Execução do Processo de Gerenciamento de Acesso e Uso de Recursos de TIC, instituído por Ato da Presidência;

V - Execução do Processo de Elaboração, Acompanhamento e Revisão da Política e Normas de Segurança da Informação, instituído por Ato da Presidência;

VI - Execução de cópias de segurança dos ativos de TIC, em conformidade com a norma e a política institucional para realização de backup de dados, instituídas por Atos da Presidência;

VII - Implementação gradual dos Manuais de Referência definidos na ENSEC-PJ:

a) Manual de Proteção de Infraestruturas Críticas de TIC;

b) Manual de Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital;

c) Manual de Gestão de Identidade e de Controle de Acessos;

d) Manual de Política de Educação e Cultura em Segurança Cibernética.

VIII - Implementação de boas práticas de gerenciamento e de proteção do

ambiente tecnológico, com base em normatizações e frameworks relacionados, como por exemplo ABNT NBR 27002 e CIS Controls.

Seção III

Das Funções Detectar, Responder e Recuperar

Art. 11. A função “Detectar” consiste no desenvolvimento e implementação de atividades adequadas à descoberta oportuna de eventos ou à detecção de incidentes de Segurança Cibernética.

Art. 12. A função “Responder” consiste no desenvolvimento e implementação de atividades apropriadas à adoção de medidas em incidentes cibernéticos detectados.

Art. 13. A função “Recuperar” consiste no 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. 14. No âmbito da instituição, as funções são contempladas pelas seguintes atividades:

I - Execução do Processo de Gestão de Incidentes de Segurança da Informação, instituído por Ato da Presidência;

II - Execução do Processo de Gestão de Continuidade de TIC, instituído por Ato da Presidência.

CAPÍTULO III

Das responsabilidades

Art. 15. As estruturas organizacionais atuantes no PPINC no âmbito da instituição são:

I - Comitê Gestor de Segurança da Informação;
II - Secretaria de Tecnologia da Informação e Comunicação;
III - Assessoria de Governança de Segurança da Informação;
IV - Assessoria de Governança de TIC;
V - Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética.

Art. 16. Demais atores poderão ser envolvidos em atividades e ações relacionadas a esse protocolo, como: Presidência do Tribunal, Comitê de Crises Cibernéticas, Comitê

Gestor de Proteção de Dados Pessoais, dentre outros.

Art. 17. As responsabilidades e atribuições referentes ao PPINC são aquelas definidas na Política de Segurança da Informação e Comunicações, na Política de Proteção de Dados Pessoais, nos processos do Sistema de Gestão de Segurança da Informação e demais instrumentos relacionados.

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art. 18. Na ocorrência de incidentes cibernéticos que envolvam ilícitos criminais, serão observadas as disposições do Protocolo de Investigação para Ilícitos Cibernéticos, em complemento ao PPINC.

Art. 19. Na ocorrência de incidentes cibernéticos que resultem em crises institucionais, serão observadas as disposições do Protocolo de Gerenciamento de Crises Cibernéticas, em complemento ao PPINC.

Art. 20. O PPINC poderá ser revisado sempre que alguma atualização for necessária, mediante aprovação do Comitê Gestor de Segurança da Informação.

Art. 21. O presente Ato entra em vigor a partir da data de sua publicação.

Dê-se ciência.
Publique-se no DEJT- Adm.

LEONARDO JOSÉ VIDERES TRAJANO

Desembargador Presidente