ATO TRT13 SGP Nº 164 DE 6 DE DEZEMBRO DE 2022

Institui o Protocolo de Investigação para Ilícitos Cibernéticos (PIILC) 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 n.º 10113/2022,

CONSIDERANDO a Resolução CNJ n.º 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Portaria CNJ n.º 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 que os ataques cibernéticos têm se tornado cada vez mais avançados e com alto potencial de prejuízo, cujo alcance e complexidade não têm precedentes; que os impactos financeiros, operacionais e de reputação podem ser

imediatos e significativos; e que é fundamental aprimorar a capacidade da instituição de coordenar pessoas, desenvolver recursos e aperfeiçoar processos, visando minimizar danos e agilizar o restabelecimento da condição de normalidade em caso de ocorrência de ataques cibernéticos de grande impacto,

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Estabelecer o Protocolo de Investigação para Ilícitos Cibernéticos (PIILC) no âmbito do Tribunal Regional do Trabalho da 13ª Região, tendo como principais objetivos:

I - Estabelecer os procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal;

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

III - Definir requisitos para adequação dos ativos de tecnologia da informação e comunicação (TIC) no que tange à configuração e ao registro de informações de auditoria.

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 - Crise cibernética: crise que ocorre em decorrência de incidente em dispositivos, serviços e redes de computadores, que cause dano material ou de imagem, atraia a atenção do público e da mídia, e fuja ao controle direto da organização;

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

III - 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;

IV - Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de Segurança da Informação em redes de computadores (Segurança Cibernética);

V - Agente Responsável: servidor público, ocupante de cargo efetivo, encarregado de coordenar a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR).

Art. 3º As ações e medidas elencadas nesse 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

DOS REQUISITOS PARA ADEQUAÇÃO DOS ATIVOS DE TIC

Art. 5º A Secretaria de Tecnologia da Informação e Comunicação (SETIC) deverá promover as ações necessárias para adequação dos ativos de TIC que suportam os serviços considerados estratégicos e essenciais ao funcionamento da instituição aos requisitos elencados no item 2 do anexo III da Portaria CNJ nº 162/2021.

Parágrafo único. A Assessoria de Governança de Segurança da Informação elaborará plano para acompanhamento das ações de adequação citadas no *caput*, o qual será encaminhado ao Comitê Gestor de Segurança da Informação e integrado ao Sistema de Gestão de Segurança da Informação (SGSI) para revisões periódicas em cada ciclo.

CAPÍTULO III

DOS PROCEDIMENTOS PARA COLETA E PRESERVAÇÃO DE EVIDÊNCIAS

Art. 6º A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR), sob a supervisão do Agente Responsável, durante o processo de tratamento do um incidente cibernético penalmente relevante, deverá, sem prejuízo de outras ações, coletar e preservar as evidências digitais necessárias ao processo de investigação a ser conduzido pela autoridade competente.

Parágrafo único. A coleta e preservação de evidências deverá ser realizada de acordo com as práticas de forense digital, sendo observados os procedimentos definidos no item 3 do anexo III da Portaria CNJ nº 162/2021, de forma a garantir a devida confidencialidade, integridade e autenticidade das informações coletadas.

CAPÍTULO IV

DA COMUNICAÇÃO

Art. 7º Após a conclusão do processo de coleta e preservação das evidências de um incidente cibernético penalmente relevante, o Agente Responsável pela ETIR deverá elaborar Relatório de Comunicação de Incidente de Segurança Cibernética descrevendo detalhadamente os eventos verificados, de acordo com os requisitos definidos no item 4 do anexo III da Portaria CNJ nº 162/2021.

Parágrafo único. O Agente Responsável pela ETIR deverá submeter formalmente o relatório ao Comitê Gestor de Segurança da Informação para encaminhamento à Presidência do Tribunal.

Art. 8º Recebida a comunicação de um incidente cibernético penalmente relevante, a Presidência do Tribunal encaminhará a mesma, formalmente, ao Ministério Público e ao órgão de polícia judiciária com atribuição para apurar os fatos, juntamente com as evidências coletadas, para fins de instrução da notícia crime.

CAPÍTULO V

DAS RESPONSABILIDADES

Art. 9º As estruturas organizacionais atuantes no PIILC no âmbito da instituição são:

I - Presidência do Tribunal;

II - Secretaria de Tecnologia da Informação e Comunicação;

III - Assessoria de Governança de Segurança da Informação;

IV - Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética - ETIR.

Art. 10. Demais atores poderão ser envolvidos em atividades e ações relacionadas a esse protocolo, como: Comitê Gestor de Segurança da Informação, Comitê Gestor de Proteção de Dados Pessoais, Comitê de Crises Cibernéticas, Encarregado pelo Tratamento de Dados Pessoais, dentre outros.

Art. 11. As responsabilidades e atribuições referentes ao PIILC 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 VI

DAS DISPOSIÇÕES FINAIS

Art. 12. Na ocorrência de incidentes cibernéticos penalmente relevantes, que resultem em crises institucionais, serão observadas as disposições do Protocolo de Gerenciamento de Crises Cibernéticas, em complemento ao PIILC**.**

Art. 13. O PIILC poderá ser revisado sempre que alguma atualização for necessária, mediante aprovação do Comitê Gestor de Segurança da Informação.

Art. 14. 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