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

Institui o Protocolo de Investigação de Ilícitos 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 12343/2021;

CONSIDERANDO a Resolução Administrativa TRT 18ª nº 145/2019, que institui a Política de Segurança da Informação do Tribunal Regional do Trabalho da 18ª Região;

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 III,

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Portaria institui o Protocolo de Investigação de Ilícitos Cibernéticos (PIILC), que estabelece os procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória ao Ministério Público Federal e ao órgão de polícia judiciária com atribuição para o início da persecução penal, relativamente a fatos penalmente relevantes no âmbito cibernético.

Parágrafo único. Aplica-se o disposto nesta Portaria ao tratamento de incidentes cibernéticos penalmente relevantes, no âmbito do Tribunal Regional do Trabalho

da 18ª Região, conduzidos pela Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR), sob supervisão de seu agente responsável.

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

Art. 3º A unidade de tecnologia da informação e comunicação deverá adequar os ativos de tecnologia da informação aos requisitos elencados no item 2 do anexo III da Portaria CNJ nº 162/2021.

Parágrafo único. A adequação a que se refere o *caput* deverá ser mantida ao longo do tempo para ativos de tecnologia da informação novos ou modificados.

CAPÍTULO II
DO PROCEDIMENTO PARA COLETA E PRESERVAÇÃO DE EVIDÊNCIAS

Art. 4º A ETIR, sob a supervisão de seu agente responsável, durante o processo de tratamento do incidente penalmente relevante, deverá, sem prejuízo de outras ações, coletar e preservar:

a) as mídias de armazenamento dos dispositivos afetados ou as suas respectivas imagens forenses;

b) os dados voláteis armazenados nos dispositivos computacionais, como a memória principal (memória RAM); e

c) todos os registros de eventos citados neste documento.

Art. 5º Nos casos de inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados ou das suas respectivas imagens forenses, em razão da necessidade de pronto restabelecimento do serviço afetado, a ETIR, sob a supervisão do seu agente responsável, deverá coletar e armazenar cópia dos arquivos afetados pelo incidente, tais como: *logs*, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original e os “metadados” desses arquivos, como data, hora de criação e permissões.

Art. 6º O agente responsável pela ETIR deverá fazer constar em relatório a eventual impossibilidade de preservação das mídias afetadas e listar todos os procedimentos adotados.

Art. 7º As ações de restabelecimento do serviço não devem comprometer a coleta e a preservação da integridade das evidências.

Art. 8º Para a preservação dos arquivos coletados, deve-se:

a) gerar arquivo que contenha a lista dos resumos criptográficos de todos os arquivos coletados;

b) gravar os arquivos coletados, acompanhados do arquivo com a lista dos resumos criptográficos descritos na alínea “a” deste artigo; e

c) gerar resumo criptográfico do arquivo a que se refere a alínea “a” deste artigo.

Art. 9º Todo material coletado deverá ser lacrado e custodiado pelo agente responsável pela ETIR, o qual deverá preencher o Termo de Custódia dos Ativos de Informação relacionados ao incidente de segurança penalmente relevante.

Art. 10. O material coletado ficará à disposição da Presidência.

CAPÍTULO III
DA COMUNICAÇÃO DO INCIDENTE DE SEGURANÇA

Art. 11. Assim que tomar conhecimento de Incidente de Segurança Cibernética penalmente relevante que afete esta eg. Corte, deverá a Presidência comunicá-lo, de imediato, ao órgão de polícia judiciária com atribuição para apurar os fatos e ao Ministério Público.

Art. 12. Considerado o incidente Crise Cibernética, o Comitê de Crise deverá ser acionado, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas.

Art. 13. Após a conclusão do processo de coleta e preservação das evidências do incidente penalmente relevante, o agente responsável pela ETIR deverá elaborar Relatório de Comunicação de Incidente de Segurança Cibernética, descrevendo detalhadamente os eventos verificados.

Art. 14. O Relatório de Comunicação de Incidente de Segurança Cibernética deverá conter as seguintes informações, sem prejuízo de outras julgadas relevantes:

a) nome do responsável pela preservação dos dados do incidente, com informações de contato;

b) nome do agente responsável pela ETIR e informações de contato;

c) órgão comunicante com sua localização e informações de contato;

d) número de controle da ocorrência;

e) relato sobre o incidente que descreva o que ocorreu, como foi detectado e quais dados foram coletados e preservados;

f) descrição das atividades de tratamento e resposta ao incidente e todas as providências tomadas pela ETIR, incluindo as ações de preservação e coleta, a metodologia e as ferramentas utilizadas e o local de armazenamento das informações preservadas;

g) resumo criptográfico dos arquivos coletados;

h) Termo de Custódia dos Ativos de Informação Relacionados ao Incidente de Segurança;

i) número de lacre de material físico preservado, se houver; e

j) justificativa sobre a eventual inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados, diante da impossibilidade de mantê-las.

Art. 15. O Relatório de Comunicação de Incidente de Segurança Cibernética deverá ser acondicionado em envelope lacrado, rubricado pelo agente responsável pela ETIR e, posteriormente, protocolado e encaminhado formalmente à Presidência.

Art. 16. Deverá constar no documento formal de encaminhamento a que se refere o artigo 15 apenas a informação de que se trata de comunicação de evento relacionado à segurança da informação, sem a descrição dos fatos.

Art. 17. Recebida a Comunicação de Incidente de Segurança Cibernética, a Presidência deverá encaminhá-la formalmente ao Ministério Público e ao órgão de polícia judiciária com atribuição para apurar os fatos, juntamente com todo o material previsto neste protocolo, para fins de instrução da notícia-crime.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 18. 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

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

DANIEL VIANA JÚNIOR

DESEMB. PRES. DE TRIBUNAL