PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO TRT7.GP Nº 143, DE 23 DE SETEMBRO DE 2021

Institui o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário no âmbito do Tribunal Regional do Trabalho da 7ª Região (TRT7).

A DESEMBARGADORA-PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a Norma Complementar 08/IN01/DSIC/GSIPR, do Gabinete de Segurança Institucional da Presidência da República, de 24 de agosto de 2010, que "estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal";

CONSIDERANDO que a Resolução nº 370, de 28 de janeiro de 2021, do Conselho Nacional de Justiça, estabelece no art. 21 (inciso II, alínea "a") a necessidade de constituir e manter estruturas organizacionais adequadas e compatíveis para o macroprocesso de "incidentes de segurança";

CONSIDERANDO a Resolução nº 396, de 07 de junho de 2021, do Conselho Nacional de Justiça, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO o anexo II da Portaria nº 162, de 10 de junho de 2021, do Conselho Nacional de Justiça, que constitui o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Poder Judiciário (PGCRC-PJ);

CONSIDERANDO a Resolução Normativa nº 14, de 22 de junho de 2020 do TRT da 7ª Região, que institui a Política de Segurança da Informação e Comunicações (POSIC) no âmbito deste Tribunal,

RESOLVE:

Art. 1º Adotar o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ), no âmbito do TRT7, nos termos deste ato.

Art. 2º O Protocolo de Gerenciamento de Crises Cibernéticas é complementar ao Protocolo de Prevenção de Incidentes Cibernéticos e prevê as ações responsivas a serem colocadas em prática quando ficar evidente que um incidente de segurança cibernética não será mitigado rapidamente e poderá durar dias, semanas ou meses.

Parágrafo único. Para os efeitos deste normativo, são estabelecidas as seguintes definições:

I - Ativos críticos: os meios de armazenamento, transmissão e processamento da informação, incluindo os equipamentos, os softwares e sistemas, os locais onde se encontram esses meios relativos às atividades consideradas estratégicas e essenciais ao funcionamento do Tribunal;

II - Crise: um evento ou série de eventos danosos que apresentam propriedades emergentes capazes de exceder as habilidades de uma organização em lidar com as demandas de tarefas geradas, e que apresentam implicações que afetam uma proporção considerável da organização, bem como de seus constituintes;

III - Crise cibernética: crise que ocorre em decorrência de incidentes em dispositivos, serviços e redes de computadores. É decorrente de incidentes que causam dano material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização.

Art. 3º São serviços de Tecnologia da Informação e Comunicação (TIC) considerados estratégicos e essenciais ao funcionamento do Tribunal para efeito deste protocolo:

I - o Sistema de Processo Judicial Eletrônico de 1º e 2º Graus;

II - o Sistema de Gestão de Pessoas/Folha de Pagamento;

III - o acesso ao Sistema Integrado de Administração Financeira do Governo Federal (SIAFI);

Art. 4º O gerenciamento de crise se inicia quando:

I - ficar caracterizado grave dano material ou de imagem;

II - restar evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses;

III - o incidente impactar gravemente os serviços de TIC essenciais ao funcionamento do Tribunal, extrapolando os limites determinados nas diretrizes do plano de continuidade de TIC do TRT7;

IV - atrair grande atenção da mídia e da população em geral;

V - ocorrer vazamento de quantidade significativa de dados pessoais;

Art. 5º A Presidência do TRT da 7ª Região encaminhará comunicado da ocorrência do incidente grave quando constatada uma crise cibernética:

I - ao Conselho Superior da Justiça do Trabalho;

II - ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), órgão superior vinculado ao Conselho Nacional de Justiça;

III - à Ordem dos Advogados do Estado do Ceará (OAB/CE), quando o incidente envolver a prestação jurisdicional.

Parágrafo único. Cabe ao encarregado(a) pelo tratamento de dados pessoais no âmbito do TRT da 7ª Região comunicar incidentes graves, quando envolver dados pessoais:

I - à Autoridade Nacional de Proteção de Dados (ANPD);

II - aos titulares de dados pessoais.

Art. 6º Fica instituído o Comitê de Crises Cibernéticas, para cumprimento das competências definidas no PGCRC/PJ, com a seguinte formação:

I - Presidente do Tribunal;

II - Vice-Presidente do Tribunal;

III - Secretário(a)-Geral da Presidência;

IV - Diretor(a) da Divisão de Comunicação Social;

V - Diretor(a)-Geral;

VI - Secretário(a) Administrativa;

VII - Secretário(a) de Tecnologia da Informação e Comunicação;

VIII - Encarregado(a) pelo tratamento de dados pessoais no Tribunal;

IX - Chefe do Gabinete de Segurança da Informação;

X - Chefe ou Diretor(a) da Divisão de Segurança e Transporte.

§ 1º O(A) Presidente do Tribunal preside o Comitê, e, na sua ausência, o(a) Vice-Presidente.

§ 2º O Comitê de Crises Cibernéticas deverá se reunir no Gabinete da Presidência (sala de situação), imediatamente à constatação de que um incidente de segurança da informação constitui uma crise cibernética.

§ 3º As reuniões do Comitê de Crises Cibernéticas poderão ser realizadas, por determinação da Presidência, em outro local ou ainda por videoconferência, excepcionalmente, na indisponibilidade da sala de situação.

Art. 7º Cabe à Secretaria de Tecnologia da Informação e Comunicação (SETIC):

I - observar o Protocolo de Prevenção a Incidentes Cibernéticos;

II - identificar e manter documentação técnica atualizada dos ativos de informação que suportam as atividades estratégicas;

III - avaliar e tratar os riscos de TIC aos quais as atividades estratégicas estão expostas e que possam impactar diretamente na continuidade do negócio, de acordo com o processo de gestão de riscos de segurança da informação;

IV - elaborar plano de gestão de incidentes cibernéticos para o ativos críticos;

V - elaborar e testar planos de contingência de TIC para os serviços essenciais dispostos no art. 3º deste ato, sem prejuízo das ações decorrentes da norma complementar que estabelece as diretrizes para a gestão da continuidade de TIC do TRT7.

Parágrafo único. As atividades previstas nos incisos II, IV e V deste artigo devem ser concluídas no prazo de 120 (cento e vinte) dias.

Art. 8º Este ato entra em vigor na data de sua publicação.

Fortaleza, 23 de setembro de 2021.
REGINA GLÁUCIA CAVALCANTE NEPOMUCENO
Presidente do Tribunal