PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 16ª REGIÃO
GABINETE DA PRESIDÊNCIA

ATO REGULAMENTAR GP/TRT16 Nº 03/2025.

Institui o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Tribunal Regional do Trabalho da 16ª Região.

A DESEMBARGADORA PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 16ª REGIÃO, no uso de suas atribuições legais e regimentais,

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

CONSIDERANDO a Recomendação CNJ nº 160, de 8 de novembro de 2024, que recomenda a todos os tribunais a adoção do Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ);

CONSIDERANDO a aprovação da proposta do Protocolo de Gerenciamento de Crises Cibernéticas pelo Comitê de Segurança da Informação e Proteção de Dados deste Tribunal,

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º Instituir o Protocolo de Gerenciamento de Crises Cibernéticas (PGCC) aplicável no âmbito do Tribunal Regional do Trabalho da 16ª Região.

Art. 2º Fica estabelecido que o Protocolo de Gerenciamento de Crises Cibernéticas (PGCC) contempla ações de preparação para lidar com crises cibernéticas. Constituem o PGCC os seguintes processos: Processo de Gestão de Risco de Segurança da Informação, Processo de Monitoramento e Respostas a Incidentes de Segurança da Informação e o Processo de Gestão de Continuidade de TIC.

CAPÍTULO II
TERMOS E DEFINIÇÕES

Art. 3º Para fins deste protocolo, aplicam-se as seguintes definições:

I - Crise Cibernética: Situação em que um ou mais incidentes de segurança da informação causam impacto significativo nos ativos críticos ou na operação institucional.

II - Ativo Crítico: Sistema, serviço ou recurso essencial para o funcionamento adequado do tribunal e que exige prioridade em sua recuperação.

III - Incidente de Segurança da Informação: Evento ou conjunto de eventos que comprometa a confidencialidade, integridade ou disponibilidade de informações e sistemas.

IV - ETIR (Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação): Equipe responsável pela identificação, contenção, mitigação e investigação de incidentes de segurança.

V - Sala de Situação: Local designado para a coordenação de ações durante uma crise cibernética.

VI - Processo de Continuidade de TIC: Documento estratégico que define ações para assegurar a continuidade das operações essenciais do Tribunal em caso de incidentes ou crises.

VII - Processo de Monitoramento e Respostas a Incidentes de Segurança da Informaçãα Documento operacional que descreve procedimentos a serem adotados em resposta a incidentes de segurança, visando à contenção, mitigação e recuperação.

VII - Processo de Gestão de Riscos de TIC: Documento que descreve ações para garantir que os riscos relacionados à segurança da informação sejam reduzidos a níveis aceitáveis, alinhados com as prioridades e os objetivos estratégicos da organização.

CAPÍTULO III
OBJETIVO

Art. 4º Este protocolo tem como objetivo estabelecer diretrizes e procedimentos para o gerenciamento de crises cibernéticas no Tribunal Regional do Trabalho da 16ª Região (TRT-16), assegurando a recuperação rápida dos ativos críticos e a continuidade dos serviços essenciais prestados pela instituição. Ele também busca garantir a proteção das informações institucionais e a minimização dos impactos causados por incidentes de segurança.

CAPÍTULO IV
ATIVOS CRÍTICOS

Art. 5º Os seguintes ativos são considerados críticos para as operações do TRT-16 e deverão ser priorizados em situação de crise cibernética:

I - PJe (Processo Judicial Eletrônico): Sistema de tramitação de processos judiciais.

II - Aud: Sistema de audiência..

III - Site do Tribunal: Plataforma oficial de comunicação com o público.

IV - SEI (Sistema Eletrônico de Informações): Sistema de gestão de processos administrativos.

V - SIGEP-JT: Sistema de gestão de pessoas.

VI - Serviço Institucional de Comunicação e Compartilhamento de Arquivos: Plataforma para troca segura de informações e arquivos institucionais.

CAPÍTULO V
ATORES ENVOLIDOS NO GERENCIAMENTO DA CRISE

Art. 6º As seguintes unidades e grupos serão responsáveis por atuar no gerenciamento da crise cibernética:

I - Comitê de Segurança da Informação e Proteção de Dados: Responsável por coordenar as ações estratégicas durante a crise.

II - Secretaria de Tecnologia da Informação e Comunicações (SETIC): Unidade responsável pela execução das ações técnicas para contenção e recuperação dos sistemas afetados.

III - Divisão de Infraestrutura e Segurança da Informação: Responsável por garantir a segurança dos ativos de TI e realizar diagnósticos técnicos.

IV - Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR): Grupo operacional encarregado de identificar, conter, mitigar e investigar incidentes de segurança da informação;

V - Divisão de Assessoria de Comunicação Social (DIVASCOM): Responsável pela comunicação oficial com a imprensa e com a sociedade.

CAPÍTULO VI
GERENCIAMENTO DA CRISE

Art. 7º A crise cibernética é oficialmente iniciada quando:

I - Um incidente de segurança da informação com impacto significativo nos ativos críticos é identificado, caracterizado por um ou mais dos seguintes critérios:

a) Grave dano material ou de imagem é constatado.

b) Evidências indicam que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses.

c) O incidente impacta a atividade finalística ou um serviço crítico mantido pela Tribunal.

d) O incidente atrai grande atenção da mídia e da população em geral.

II - O Comitê de Segurança da Informação e Proteção de Dados decide formalmente pela ativação do protocolo de gerenciamento de crise.

Parágrafo único: A ativação será comunicada a todos os atores envolvidos e ao Presidente do Tribunal, que dará aval para a mobilização das equipes.

Art. 8º A crise será considerada finalizada quando:

I - Todos os ativos críticos afetados forem plenamente recuperados e estiverem operacionais.

II - Os impactos no funcionamento do tribunal forem mitigados.

III - Um relatório final detalhado do incidente, com as ações tomadas e recomendações futuras for apresentado pelo Comitê de Segurança da Informação e Proteção de Dados à Presidência do Tribunal.

CAPÍTULO VII
SALA DE SITUAÇÃO

Art. 9º A sala de situação será instalada no Gabinete da Presidência do Tribunal, que funcionará como o centro

de coordenação de ações e tomada de decisões durante o período de crise.

CAPÍTULO VIII
DISPOSIÇÕES FINAIS

Art. 10º Este Ato entra em vigor na data de sua publicação.

Dê-se ciência.

Publique-se no Diário Eletrônico da Justiça do Trabalho e disponibilize-se no Sítio Eletrônico do Tribunal.

São Luís (MA), datado e assinado eletronicamente.

Desembargadora MÁRCIA ANDREA FARIAS DA SILVA
Presidente do Tribunal Regional do Trabalho da 16ª Região

TRT-16ª REGIÃO
Gabinete da Presidência

Av. Senador Vitorino Freire, nº 2001, Areinha, 6º Andar
CEP 65030-015 – São Luís - Maranhão
(98) 2109-9306 / presidencia@trt16.jus.br

Documento assinado eletronicamente por **MÁRCIA ANDREA FARIAS DA SILVA**, **Presidente**, em 24/02/2025, às 11:22, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site Autenticar Documentos informando o código verificador **0217647** e o código CRC **8B5C4E1E**.

Referência: Processo nº 000007673/2024 SEI nº 0217647