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

Institui o Protocolo de Gerenciamento de Crises Cibernéticas 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 12803/2021;

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 II;

CONSIDERANDO a Resolução Administrativa TRT 18ª nº 145/2016, que institui a Política de Gestão de Continuidade de Negócios do Tribunal Regional do Trabalho da 18ª Região,

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Portaria institui o Protocolo de Gerenciamento de Crises Cibernéticas (PGCRC) aplicável no âmbito do Tribunal Regional do Trabalho da 18ª Região.

§ 1º 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.

§ 2º A Gestão de Crises Cibernéticas é realizada no contexto do Plano de Gestão de Crises - PGC do TRT da 18ª Região.

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

CAPÍTULO II
DA IDENTIFICAÇÃO DE CRISE CIBERNÉTICA

Art. 3º Durante o tratamento e resposta a um incidente cibernético, ativar-se-á o gerenciamento de crise 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 a atividade finalística ou o serviço crítico mantido pelo Tribunal; ou

IV – o incidente atrair grande atenção da mídia e da população em geral.

CAPÍTULO III
DO PLANEJAMENTO - PRÉ-CRISE

Art. 4º A preparação para crises cibernéticas é realizada por meio do programa de gerenciamento de continuidade de serviços essenciais de TIC, que deve contemplar as seguintes atividades:

I – observar o Protocolo de Prevenção a Incidentes Cibernéticos do TRT da 18ª Região;

II – definir as atividades críticas que são fundamentais para a atividade finalística do Tribunal;

III – identificar os ativos de informação críticos, ou seja, aqueles que suportam as atividades primordiais, incluindo as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação;

IV – avaliar continuamente os riscos a que as atividades críticas estão expostas e que possam impactar diretamente na continuidade do negócio;

V – categorizar os incidentes e estabelecer procedimentos de resposta

específicos (*playbooks*) para cada tipo de incidente, de forma a apoiar equipes técnicas e de liderança em casos de incidentes cibernéticos;

VI – priorizar o monitoramento, acompanhamento e tratamento dos riscos de maior criticidade. Tais atividades deverão ser detalhadas e consolidadas em um plano de contingência que contemple diversos setores, em razão de possíveis cenários de crise, a fim de se contrapor à escalada de uma eventual crise e com o objetivo de manter os serviços prestados pelo Tribunal; e

VII – realizar simulações e testes para validação dos planos e procedimentos.

Art. 5º A Equipe de Gerenciamento de Crises, estabelecida no Plano de Gestão de Crises deste Regional, atuará como Comitê de Crises Cibernéticas e será suportada tecnicamente pela Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética - ETIR e por especialistas:

I – da área Jurídica;

II – da área de Comunicação Institucional;

III – da área de Tecnologia da Informação e Comunicação;

IV – da área de Privacidade de Dados Pessoais;

V – da área de Segurança da Informação;

VI – das unidades administrativas de apoio à contratação; e

VII – da área de Segurança Institucional.

Art. 6º Um local de reunião da Equipe de Gerenciamento de Crises, também conhecido como “sala de situação”, é definido no âmbito do Plano de Gestão de Crises desta Instituição.

Art. 7º O Plano de Gestão de Incidentes Cibernéticos deve possuir, no mínimo, as categorias de incidentes a que os ativos críticos estão sujeitos, a indicação do procedimento de resposta específico a ser aplicado em caso de ocorrência do incidente e a severidade do incidente.

Parágrafo único. Um exemplo de Plano de Gestão de Incidentes Cibernéticos é apresentado no Anexo I.

CAPÍTULO IV
DA EXECUÇÃO - DURANTE A CRISE

Art. 8º Para que o TRT da 18ª Região reaja a uma crise cibernética de longa duração ou de grande impacto, é fator fundamental a comunicação entre as áreas envolvidas.

Art. 9º Assim que a ETIR identificar que um incidente constitui uma crise cibernética, a Equipe de Gerenciamento de Crises deverá se reunir imediatamente na “sala de situação” definida no âmbito do Plano de Gestão de Crises.

Art. 10. Os planos de contingência existentes, caso aplicáveis, devem ser efetivados imediatamente, visando à continuidade dos serviços prestados.

Art. 11. O Plano de Gestão de Crises define a chefia da Equipe de Gerenciamento de Crises e suas respectivas atribuições.

Art. 12. A “sala de situação” é o local a partir do qual serão geridas as situações de crise, devendo dispor dos meios necessários (ex.: sistemas de áudio, vídeo, chamadas telefônicas) e estar preferencialmente próxima a um local onde se possa fazer declarações públicas à imprensa e com acesso restrito à Equipe de Gerenciamento de Crises e a outros entes eventualmente convidados a participar das reuniões.

Art. 13. A “sala de situação” deve ser um ambiente que permita à Equipe de Gerenciamento de Crises deliberar com tranquilidade e que possua uma equipe dedicada à execução de atividades administrativas para o período da crise.

Art. 14. Para eficácia do trabalho, é necessário a Equipe de Gerenciamento de Crises:

I – entender claramente o incidente que gerou a crise, sua gravidade e os impactos negativos;

II – levantar todas as informações relevantes, verificando fatos e descartando boatos;

III – levantar soluções alternativas para a crise, avaliando sua viabilidade e consequências;

IV – avaliar a necessidade de suspender serviços e/ou sistemas informatizados;

V – centralizar a comunicação na figura de um porta-voz para evitar informações equivocadas ou imprecisas;

VI – realizar comunicação tempestiva e eficiente, de forma a evidenciar o trabalho diligente das equipes e a enfraquecer boatos ou investigações paralelas que alimentem notícias falsas;

VII – definir estratégias de comunicação com a imprensa e/ou redes sociais e estabelecer qual a mídia mais adequada para se utilizar em cada caso;

VIII – aplicar o Protocolo de Investigação de Ilícitos Cibernéticos do Tribunal Regional do Trabalho da 18ª Região;

IX – solicitar a colaboração de especialistas ou de centros de resposta a incidentes de segurança;

X – apoiar equipes de resposta e de recuperação com gerentes de crise experientes;

XI – avaliar a necessidade de recursos adicionais extraordinários a fim de apoiar as equipes de resposta;

XII – orientar sobre as prioridades e estratégias do Tribunal para recuperação rápida e eficaz;

XIII – definir os procedimentos de compartilhamento de informações relevantes para a proteção de outras organizações com base nas informações colhidas sobre o incidente; e

XIV – elaborar plano de retorno à normalidade.

Art. 15. As etapas e os procedimentos de resposta são diferentes a depender do tipo de incidente de segurança causador da crise. Dessa forma, são necessárias reuniões regulares para avaliar o progresso até que seja possível retornar à condição de normalidade.

Art. 16. Todos os incidentes graves deverão ser comunicados ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), órgão superior vinculado ao Conselho Nacional de Justiça.

Parágrafo único. Em caso de impossibilidade de comunicação ao CPTRIC-PJ, os incidentes deverão ser comunicados ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), vinculado ao Poder Executivo.

Art. 17. Incidentes envolvendo dados pessoais deverão ser comunicados à Agência Nacional de Proteção de Dados - ANPD e aos respectivos titulares, na forma da Lei 13.709/2018 e das demais regulamentações específicas.

CAPÍTULO V
DA MELHORIA CONTÍNUA - PÓS-CRISE

Art. 18. Após o retorno das operações à normalidade, a Equipe de Gerenciamento de Crises deverá realizar a análise criteriosa das ações tomadas,

observando as que foram bem-sucedidas e as que ocorreram de forma inadequada.

Art. 19. Para a identificação das lições aprendidas e a elaboração de relatório final, devem ser objeto de avaliação:

I – a identificação e análise da causa-raiz do incidente;

II – a linha do tempo das ações realizadas;

III – a escala do impacto nos dados, sistemas e operações de negócios importantes durante a crise;

IV – os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas;

V – o escalonamento da crise;

VI – a investigação e preservação de evidências;

VIII – a efetividade das ações de contenção;

IX – a coordenação da crise, liderança das equipes e gerenciamento de informações; e

X – a tomada de decisão e as estratégias de recuperação.

Art. 20. As lições aprendidas devem ser utilizadas para a elaboração ou revisão dos procedimentos específicos de resposta (*playbooks*) e para a melhoria do processo de preparação para crises cibernéticas.

Art. 21. Deve ser elaborado Relatório de Comunicação de Incidente de Segurança Cibernética, que contenha a descrição e o detalhamento da crise, bem como o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 22. 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

Anexo I

Exemplo de Plano de Gestão de Incidentes Cibernéticos

Item	Indicação do incidente cibernético	Descrição	Procedimento	Severidade
1	Campanha de phishing	O órgão é alvo de uma campanha de phishing.	Identificação do documento de procedimento de resposta específico.	Média
2	Degradação de serviços	Degradação ou interrupção de serviços ou sistemas por ataque de negação de serviço (DoS).	Identificação do documento de procedimento de resposta específico.	Alta
3	Comprometimento de credenciais	Comprometimento de credenciais com acesso a informações sensíveis.	Identificação do documento de procedimento de resposta específico.	Alta
4	Impossibilidade de acesso à informação	Importantes informações organizacionais inacessíveis por encriptação (ransomware).	Identificação do documento de procedimento de resposta específico.	Crítica
5	Vazamento de informação e dados pessoais	Informações críticas encontradas fora da organização.	Identificação do documento de procedimento de resposta específico.	Crítica

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

DANIEL VIANA JÚNIOR

DESEMB. PRES. DE TRIBUNAL