PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO

PROTOCOLO DE GERENCIAMENTO DE CRISES CIBERNÉTICAS (PGCRC-PJ)

1. OBJETIVOS

1.1. Estabelecer um conjunto de diretrizes para responder efetivamente a crises decorrentes de incidentes cibernéticos.

1.2. Promover adequação e alinhamento às regulamentações, normas e melhores práticas relacionadas à segurança cibernética.

2. CONSIDERAÇÕES IMPORTANTES

2.1. Este protocolo é parte do conjunto de Protocolos de Segurança Cibernética, definido pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), do qual também fazem parte o Protocolo de Prevenção de Incidentes Cibernéticos e o Protocolo para Investigação de Ilícitos Cibernéticos.

2.2. As ações e medidas elencadas neste protocolo são complementares às políticas, aos processos, às práticas e aos procedimentos relacionados à segurança da informação já formalizados e estabelecidos no âmbito do TRT.

2.3. Este protocolo deve ser acionado nos casos em que as medidas estabelecidas no Protocolo de Prevenção de Incidentes Cibernéticos não forem suficientes para evitar a ocorrência de um incidente.

2.4. Para efeitos deste protocolo, são considerados críticos para o funcionamento do Tribunal os seguintes sistemas:

2.4.1. PJe

2.4.2. AUD4

2.4.3. Novajus4

2.4.4. Portal www

2.4.5. SIGEP-JT (módulos FOLHA e CADASTRO)

2.4.6. PROAD

2.4.7. Google Suite

2.5. Uma crise cibernética se configura na ocorrência de 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 que eles geram e que apresentam implicações que afetam uma proporção considerável da organização, bem como de seus constituintes, afetando diretamente ou indiretamente os sistemas críticos do Tribunal.

2.6. Os atores atuantes ativamente no gerenciamento de crises cibernéticas do TRT, cujas instituições e atribuições estão definidas na Política de Segurança do TRT (Portaria GP.TRT4 nº 4.772/2008), Regimento Interno e demais portarias relacionadas, são os seguintes:

2.6.1. Comitê de Segurança da Informação e Proteção de Dados;

2.6.2. Secretaria-Geral de Tecnologia e Inovação;

2.6.3. Coordenadoria de Segurança da Informação e Proteção de Dados;

2.6.4. Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação.

3. GLOSSÁRIO

3.1. Os conceitos utilizados neste protocolo têm como embasamento a definição constante no Anexo VIII da Portaria CNJ nº 162/2021.

4. GERENCIAMENTO DE CRISES CIBERNÉTICAS

4.1. O gerenciamento de crise cibernética se inicia quando:

4.1.1. ficar caracterizado grave dano material ou de imagem;

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

4.1.3. 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 Tribunal;

4.1.4. atrair grande atenção da mídia e da população em geral; ou

4.1.5. ocorrer incidente de segurança com dados pessoais.

4.2. Confirmada a crise cibernética, o Comitê de Segurança da Informação e Proteção de Dados deverá se reunir, observando as definições da Portaria GP.TRT4 nº 4.347/2022.

4.2.1. Cabe ao Comitê o reporte da crise ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ).

4.2.2. Caso a crise envolva dados pessoais, o Encarregado de Tratamento de Dados Pessoais do Tribunal deve informar as entidades externas nos termos da LGPD e das demais normativas relacionadas à proteção de dados pessoais vigentes no TRT.

4.2.3. Caso a crise envolva dados pessoais, o Comitê de Segurança da Informação e Proteção de Dados deve notificar o Subcomitê de Proteção de Dados Pessoais.

4.3. Para o tratamento do incidente que ocasionou a crise, deverão ser utilizadas políticas, planos de resposta a incidentes, planos de continuidade e de recuperação de desastres e procedimentos técnicos já elaborados e formalizados.

4.3.1. Deverá ser observado o processo de gestão de incidentes de segurança da informação, estabelecido no Anexo 8 da Política de Segurança da Informação.

4.4. A crise encerra-se no momento em que for constatado o retorno à normalidade das operações.

4.4.1. Deve ser elaborado um relatório da crise com o intuito de registrar as ações que foram efetivas e as melhorias necessárias para corrigir as causas do incidente que originou a crise (lições aprendidas). O relatório deve conter as seguintes informações:

4.4.1.1. a identificação e análise da causa-raiz do incidente;

4.4.1.2. a linha do tempo das ações realizadas;

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

4.4.1.4. os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas;

4.4.1.5. as ações realizadas para tratamento da crise e avaliação de sua eficácia.

5. CONSIDERAÇÕES FINAIS

5.1. Na ocorrência de indícios de ilícitos criminais durante o tratamento de incidentes cibernéticos, além das ações elencadas ou referenciadas neste protocolo, deverá ser observado o Protocolo de Investigação de Ilícitos Cibernéticos.

5.2. Este documento deve ser revisado anualmente ou quando houver alteração significativa que enseje sua pronta alteração.