TRT 15ª REGIÃO

Secretaria de Tecnologia da Informação e Comunicações

# PROPOSTA
# Protocolo de Gerenciamento de Crises Cibernéticas (PGCRC-TRT15)

## 1 Objetivo

Este protocolo estabelece as diretrizes para promover efetiva resposta a crises decorrentes de incidentes cibernéticos no âmbito do TRT15, alinhado às regulamentações, normas e melhores práticas relacionadas à segurança cibernética.

## 2 Abrangência

O protocolo tem abrangência em todo o Tribunal Regional do Trabalho da 15ª Região.

## 3 Referências legais e normativas

Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14.08.2009, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

Norma Complementar nº 08/IN01/DSIC/GSIPR, de 14.08.2010, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais – ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

Norma Complementar nº 21/IN01/DSIC/GSIPR, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização.

Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.

Resolução Administrativa nº 023/2018, de 14 de dezembro de 2018, que dispõe sobre a Gestão de Segurança da Informação (GSI) no âmbito deste Tribunal, conduzida pelo Comitê de Governança de Segurança da Informação (CGSI).

Resolução CNJ 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

Portaria GP nº 032/2022, de 8 de fevereiro de 2022, que institui e designa os membros do Comitê Gestor de Crises do Tribunal Regional do Trabalho para apoio à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR).

# 4 Diretrizes

## *4.1 Disposições gerais*

4.1.1 A implementação do Protocolo de Gerenciamento de Crises Cibernéticas (PGCRC-TRT15) deverá ser realizada de maneira progressiva, controlada, prévia e amplamente divulgada aos usuários, visando o menor impacto para o ambiente de TIC da Instituição.

4.1.2 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.

4.1.3 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.

4.1.4 As ações deste protocolo são complementares às políticas, às normas, aos processos de trabalho, às práticas e aos procedimentos relacionados à Segurança da Informação do TRT15.

4.1.5 A estrutura de Segurança da Informação definida na Resolução Administrativa nº 023/2018 serve de base para este protocolo.

4.1.6 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 e quando ficar evidente que este incidente não será mitigado rapidamente, podendo durar dias, semanas ou meses.

4.1.7 Para efeitos deste protocolo, são considerados críticos para o funcionamento do Tribunal os sistemas previstos em portaria específica, publicada na página do Comitê Gestor de Governança da Segurança da Informação (CGSI ( na página encontrada na intranet do TRT15, em “Aplicações da Intranet / Sistemas Administrativos / Comitês e Comissões / Comitê de Governança de Segurança da Informação (CGSI)” ).

4.1.8 Uma crise cibernética se inicia na ocorrência de um evento ou série de eventos danosos, que apresentam a possibilidade de exceder os recursos e habilidades de uma organização em lidar com as demandas de tarefas que eles geram, de forma que afetam uma proporção considerável da organização, bem como de seus constituintes, prejudicando diretamente ou indiretamente os sistemas críticos do Tribunal.

4.1.9 Os atores envolvidos na prevenção a incidentes cibernéticos são os seguintes:

- Comitê Gestor de Crises (CGC);
- Comitê de Governança da Segurança da Informação (CGSI);

- Secretaria de Tecnologia da Informação e Comunicações (SETIC);
- Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR);
- Comitê Gestor de Proteção de Dados Pessoais;
- dentre outros.

## *4.2 Gerenciar Crises Cibernéticas*

4.2.1 O gerenciamento de crise cibernética se inicia quando:

- se caracterizar grave dano material ou de imagem;
- se tornar evidente que as ações de resposta ao incidente cibernético provavelmente irão persistir por longo período, podendo se estender por dias, semanas ou meses;
- o incidente impactar gravemente os serviços de TIC essenciais ao funcionamento do Tribunal, extrapolando os limites determinados nas diretrizes do Plano de Continuidade de Serviços de TIC do Tribunal;
- atrair grande atenção da mídia e da população em geral;
- ocorrer incidente de segurança com dados pessoais;

4.2.2 Confirmada a crise cibernética, o Comitê Gestor de Crises (CGC) deverá se reunir e iniciar as suas tratativas, conforme estabelecido na portaria que constituiu o referido comitê.

4.2.3 O Comitê deve reportar a crise ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ).

4.2.4 Se a crise acarreta prejuízos a 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 TRT15.

4.2.5 O tratamento da crise envolve a utilização das políticas, planos de resposta a incidentes, planos de continuidade e de recuperação de desastres e procedimentos técnicos estabelecidos no âmbito do Tribunal.

4.2.6 A crise se encerra quando as operações retornam à sua normalidade.

4.2.7 A crise deve ser registrada em relatório, de forma a manter as ações que foram efetivas e buscar evoluções para evitar/minimizar as causas do incidente origem da crise. O relatório deve conter as seguintes informações: a identificação e análise da causa-raiz do incidente; as ações realizadas e avaliação de sua eficácia; sistemas e operações impactados durante a crise; os mecanismos e processos de detecção/proteção existentes; propostas para melhorias identificadas;

### *4.3 Revisão e aprimoramento*

4.3.1 Este documento deve ser revisado anualmente ou a qualquer momento em caso de necessidade detectada.