



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

## ANEXO ÚNICO

### **PROTOCOLO DE PREVENÇÃO A INCIDENTES CIBERNÉTICOS** **(PPINC-PJ)**

#### **1. OBJETIVOS**

- 1.1. Estabelecer um conjunto de diretrizes para a prevenção de incidentes cibernéticos.
- 1.2. Promover adequação e alinhamento às regulamentações, normas e melhores práticas relacionadas à segurança cibernética.
- 1.3. Promover ações pró-ativas que contribuam para a prevenção de incidentes cibernéticos e também para a resiliência do ambiente tecnológico do Tribunal.

#### **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 Gerenciamento de Crises Cibernéticas 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. Os atores atuantes ativamente na gestão de segurança cibernética no âmbito 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:
  - 2.3.1. Comitê de Segurança da Informação e Proteção de Dados;
  - 2.3.2. Secretaria-Geral de Tecnologia e Inovação;
  - 2.3.3. Coordenadoria de Segurança da Informação e de Proteção de Dados;





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

2.3.4. Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação;

2.4. Demais atores poderão ser envolvidos em atividades e ações relacionadas à gestão de segurança cibernética como: Presidência, Subcomitê de Proteção de Dados Pessoais, dentre outros.

### 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. FUNÇÕES DO PROTOCOLO

4.1. Com base na ENSEC-PJ, as funções básicas que compõem este protocolo são: identificar, proteger, detectar, responder e recuperar.

4.1.1. A função **identificar** consiste em atividades para identificar ativos tecnológicos críticos, levantar, analisar e avaliar os riscos aos quais o ambiente tecnológico está exposto, possibilitando a priorização e concentração de recursos humanos, tecnológicos e financeiros de acordo com a criticidade. No âmbito do TRT4, a função é contemplada pela seguinte atividade:

4.1.1.1. Gestão de Riscos de Segurança da Informação, formalizada na [Política da Segurança da Informação](#) por meio do Anexo 6, e cujo [processo](#) foi definido por meio da Portaria GP.TRT4 nº 6.137/2014.

4.1.2. A função **proteger** consiste no desenvolvimento e implementação de controles que assegurem a proteção do ambiente tecnológico, dados (inclusive pessoais), além de contribuir para a eficiência e eficácia da prestação de serviços. No âmbito do TRT4, a função é contemplada pelas seguintes atividades:

4.1.2.1. Execução contínua do Sistema de Gestão de Segurança da Informação, cujo [processo](#) foi instituído por meio da Portaria GP.TRT4 nº 5.324/2023.





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

- 4.1.2.2. Gestão de Continuidade de TIC, formalizada na [Política da Segurança da Informação](#) por meio do Anexo 10, e cujo [processo](#) foi definido por meio da Portaria GP.TRT4 nº 6.137/2014.
- 4.1.2.3. Gerenciamento da Disponibilidade e Capacidade de TIC, cujo [processo](#) foi instituído por meio da Portaria GP.TRT4 nº 6.969/2017.
- 4.1.2.4. [Processo](#) de Mudança e Liberação de Serviços, instituído por meio da Portaria GP.TRT4 nº 2.628/2016.
- 4.1.2.5. Normatização do Uso dos Recursos de TI e controle de acesso, formalizada na [Política da Segurança da Informação](#) por meio do Anexo 3.
- 4.1.2.6. Realização de cópias de segurança do ambiente tecnológico, formalizada na [Política da Segurança da Informação](#) por meio do Anexo 4.
- 4.1.2.7. Implementação de boas práticas de gerenciamento e proteção do ambiente tecnológico, observado normatizações e frameworks estabelecidos no mercado (como ABNT NBR 27002:2022 e CIS *Controls*), tais como:
  - 4.1.2.7.1. Gerenciamento de vulnerabilidades;
  - 4.1.2.7.2. Implementação de soluções de segurança do ambiente tecnológico;
  - 4.1.2.7.3. *Hardening* de serviços e de sistemas.
- 4.1.2.8. Adequação gradual aos seguintes Manuais de Referência, juntos com a ENSEC-PJ, observando a aplicabilidade de cada controle ao ambiente e maturidade do TRT4 em relação à segurança cibernética: Proteção de Infraestruturas Críticas de TIC e Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital.
- 4.1.3. A função **detectar** consiste no desenvolvimento e aplicação de medidas para identificação de eventos e/ou incidentes de segurança





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

cibernética. A função **responder** consiste na definição e implementação de medidas para responder com eficiência e eficácia a incidentes de segurança cibernética. A função **recuperar** consiste no desenvolvimento, implementação e manutenção de planos e ações para prover resiliência e capacidade de recuperação aos serviços, sistemas e ativos tecnológicos quando da ocorrência de eventos e/ou incidentes de segurança cibernética. Essas três funções estão contempladas pelas seguintes atividades:

- 4.1.3.1. Gestão de Incidentes de Segurança da Informação, formalizada na [Política da Segurança da Informação](#) por meio do Anexo 8, e cujo [processo](#) foi definido por meio da Portaria GP.TRT4 nº 7.791/2015.
- 4.1.3.2. Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação, formalizada na [Política da Segurança da Informação](#) por meio do Anexo 7.
- 4.1.3.3. Gestão de Continuidade de TIC, formalizada na [Política da Segurança da Informação](#) por meio do Anexo 10, e cujo [processo](#) foi definido por meio da Portaria GP.TRT4 nº 6.137/2014.

## **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.

