



ANEXO VI

Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação – ETIR

1. Objetivos

- 1.1. Estabelecer as diretrizes para o funcionamento da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR) do Tribunal Regional do Trabalho da 4ª Região.

2. Motivações

- 2.1. Alinhamento às normas, regulamentações e melhores práticas, relacionadas à matéria.
- 2.2. Necessidade de formalização da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR) e seu funcionamento.
- 2.3. Proteção do ambiente tecnológico do Tribunal.

3. Referências Normativas

- 3.1. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação e Comunicações na Administração Pública Federal.
- 3.2. 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.
- 3.3. 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.
- 3.4. Norma Técnica ISO/IEC 27000:2018, que especifica conceitos e definições



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

relacionados às normas de segurança da informação.

- 3.5. Norma ABNT NBR ISO/IEC 27002:2022, que fornece um conjunto de referência de controles genéricos de segurança da informação.
- 3.6. Resolução CNJ nº 396, de 07 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).
- 3.7. Ato conjunto TST.CSJT.GP N.º 41, de 25 de julho de 2025, que Institui o Processo de Comunicação de Incidentes Cibernéticos na Justiça do Trabalho (PCIC).

4. Conceitos e definições

- 4.1. Artefato malicioso: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores.
- 4.2. Comunidade ou Público Alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas pela Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação.
- 4.3. CPTRIC-PJ: Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário, que tem por objetivo prover canal oficial de ações preventivas e corretivas, em caso de ameaças ou de ataques cibernéticos.
- 4.4. CTIR.GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações - DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI.
- 4.5. Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação – ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança da informação.
- 4.6. Incidente de segurança da informação: Um único ou uma série de eventos indesejados ou inesperados de segurança da informação que têm uma probabilidade significativa de colocar em perigo as operações da instituição e ameaçar a segurança da informação.
- 4.7. Tratamento de Incidentes de Segurança da Informação: conjunto de processos



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

para detectar, relatar, avaliar, responder, lidar e aprender com incidentes de segurança da informação.

4.8. Usuários: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários, e outras pessoas que se encontrem a serviço da Justiça do Trabalho, utilizando em caráter temporário os recursos tecnológicos do TRT.

4.9. Vulnerabilidade: fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças.

5. Missão da ETIR

5.1. Prover capacidade adequada para prevenção, resposta e tratamento de incidentes de segurança da informação e de dados pessoais no âmbito do TRT4.

6. Público-alvo

6.1. O público-alvo da ETIR é formado por todos os usuários do ambiente tecnológico deste Tribunal.

6.2. A ETIR relaciona-se, internamente, com as diversas unidades da Secretaria-Geral de Tecnologia e Inovação e com o Comitê de Segurança da Informação e Proteção de Dados.

6.3. Externamente, a ETIR se relaciona com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR.GOV), Polícia Federal, Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (CPTRIC-PJ) do CNJ, dentre outros.

7. Modelo de Implementação

7.1. A ETIR será composta por servidores da Secretaria-Geral de Tecnologia e Inovação, que, além de suas funções regulares, desempenharão as atividades relacionadas à prevenção, ao tratamento e à resposta a incidentes de segurança da informação e de dados pessoais.

8. Estrutura Organizacional e Composição

8.1. A ETIR é subordinada à Secretaria-Geral de Tecnologia e Inovação e é



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

coordenada pela Coordenadoria de Segurança da Informação e Proteção de Dados.

8.2. A ETIR é composta por servidores da Secretaria-Geral de Tecnologia e Inovação, sendo:

- o(a) Coordenador(a) da Coordenadoria de Segurança da Informação e Proteção de Dados;
- o(a) Coordenador(a) da Coordenadoria de Desenvolvimento de Sistemas;
- o(a) Coordenador(a) da Coordenadoria de Implantação de Sistemas;
- o(a) Coordenador(a) da Coordenadoria de Serviços de Tecnologia da Informação e Comunicações;
- o(a) Chefe da Divisão de Banco de Dados e Servidores de Aplicação;
- o(a) Chefe da Divisão de Redes e Telecomunicações;
- o(a) Chefe da Divisão de Operações de TI;
- o(a) Chefe da Divisão de Infraestrutura Básica.

8.3. Para cada uma das posições o substituto formalmente designado será o suplente;

8.4. Caso necessário, deverão ser convocados outros servidores da Secretaria-Geral de Tecnologia e Inovação e/ou servidores de outras áreas do Tribunal (jurídica, gestão de pessoas, comunicação social, etc.) para auxiliar a equipe no desenvolvimento de suas atividades.

9. Autonomia

9.1. A autonomia da ETIR é compartilhada. A equipe recomendará, no mínimo, aos gestores da Secretaria-Geral de Tecnologia e Inovação, os procedimentos de prevenção, de tratamento e de resposta a serem executados e/ou as medidas de recuperação durante um ataque e apresentará as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas). De acordo com a gravidade do incidente, a proposição deverá, ainda, ser submetida ao Comitê de Segurança da Informação e Proteção de Dados e/ou à Presidência do Tribunal. As ações serão sempre definidas em conjunto com as instâncias consultadas.

10. Atribuições



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

- 10.1. Planejar, em conjunto com outras áreas da SGTI, ações para a prevenção de incidentes cibernéticos e de dados pessoais.
- 10.2. Responder e tratar os incidentes de segurança da informação e de dados pessoais no âmbito do TRT4.
- 10.3. Receber e analisar as informações sobre vulnerabilidades, artefatos maliciosos e tentativas de intrusão, com definição de estratégias e ações para sua detecção ou correção;
- 10.4. Fornecer informações, aos envolvidos, sobre a ocorrência e, ao público interno, orientações de prevenção de incidentes de segurança da informação.
- 10.5. Manter os registros dos incidentes de segurança da informação e de dados pessoais no âmbito do TRT4.
- 10.6. Divulgar alertas ou advertências diante da ocorrência de um incidente de segurança da informação ou de dados pessoais ou, de forma proativa, em face de vulnerabilidades e incidentes conhecidos e que possam gerar impactos nas atividades dos usuários.
- 10.7. Interagir com outras equipes e órgãos relacionados ao tratamento de incidentes de segurança, participação em fóruns e redes nacionais e internacionais.

11. Atualização da Norma

- 11.1. O disposto na presente norma será atualizado sempre que alterados os procedimentos de controle de acesso à internet, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.