# DOCUMENTO DE CONSTITUIÇÃO DA ETIR

## 1 OBJETIVO

Instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) no TRT 18ª Região.

## 2 REFERÊNCIA NORMATIVA

**2.1** Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14/08/2009, doravante denominada **NC05** – Trata da Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais no âmbito da Administração Pública Federal.

**2.2** PO01 - Política de Segurança da Informação e Comunicação do TRT18.

## 3 DEFINIÇÕES

**3.1 Agente Responsável:** Servidor Público, ocupante de cargo efetivo do TRT 18ª Região, incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

**3.2 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.

**3.3 Comunidade ou Público Alvo:** é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

**3.4 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.

**3.5 Detecção de Intrusão**: é o serviço que consiste na análise do histórico de

dispositivos que detectam as tentativas de intrusões em redes de computadores, com vistas a identificar e iniciar, mediante autorização, os procedimentos de resposta a incidentes de segurança em redes computacionais, com base em eventos com caraterísticas pré-definidas, que possam levar a uma possível intrusão e, ainda, possibilitar envio de alerta em consonância com o padrão de comunicação previamente definido entre ETIR (TRT 18ª Região) e o CTIR GOV.

**3.6 Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR:** grupo de pessoas com responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes computacionais.

**3.7 Incidente de segurança**: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

**3.8 Serviço:** é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da ETIR.

**3.9 Supervisor**: Chefe imediato.

**3.10 Tratamento de Artefatos Maliciosos**: é o serviço que consiste em receber informações ou cópia de artefato malicioso que foi utilizado no ataque, ou em qualquer atividade desautorizada ou maliciosa. Uma vez recebido, o mesmo deve ser analisado, ou seja, deve-se buscar a natureza do artefato, seu mecanismo, versão e objetivo, para que seja desenvolvida, ou pelo menos sugerida, uma estratégia de detecção, remoção e defesa.

**3.11 Tratamento de Incidentes de Segurança em Redes Computacionais:** é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

**3.12** Tratamento de Vulnerabilidades: é o serviço que consiste em receber informações sobre vulnerabilidades, quer sejam em *hardware* ou *software*, objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção.

## 4 MISSÃO

É missão da ETIR prestar o serviço de Tratamento de Incidentes de Segurança em

Redes Computacionais, em caráter prioritário.

## 5 COMUNIDADE OU PÚBLICO ALVO

**5.1** A ETIR atenderá diretamente todas as unidades da STI, preferencialmente por convocação ou chamado registrado eletronicamente.

**5.2** Atenderá indiretamente, por meio do serviço de atendimento a usuários da unidade de Atendimento ao Usuário de TIC, todos os usuários da rede de computadores e de sistemas do TRT 18ª Região que registrarem eventos identificados como incidentes de segurança.

## 6 MODELO DE IMPLEMENTAÇÃO

**6.1** A ETIR será estabelecida segundo o Modelo 1, da NC05, e será formada por membros das unidades da Secretaria de Tecnologia da Informação e Comunicação (STI), preferencialmente servidores efetivos, que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais.

## 7 ESTRUTURA ORGANIZACIONAL

**7.1** A ETIR será formada por, no mínimo, os sequintes integrantes:

**7.1.1** Três servidores da unidade de Infraestrutura de TIC, um deles designado Agente Responsável;

**7.1.2** Um servidor da unidade de Atendimento ao Usuário de TIC;

**7.1.3** Um servidor da unidade de Sistemas;

**7.1.4** Um servidor da unidade de Banco de Dados;

**7.1.5** Um servidor da unidade de Segurança da Informação, cuja atuação será limitada às atividades descritas no item 5.6 do normativo NO06 – Gerenciamento de incidentes de Segurança da Informação.

**7.2** Ao Agente Responsável caberá criar os procedimentos internos, treinar os integrantes, gerenciar as atividades, distribuir tarefas para a equipe, inclusive as de caráter proativo e interfacear a comunicação com o CTIR GOV.

**7.3** Seus integrantes serão indicados pelo Diretor da STI e designados por meio de portaria DG/GP.

## 8 AUTONOMIA DA ETIR

**8.1** A ETIR seguirá o modelo “Sem Autonomia” da NC05, em que só poderá agir com autorização do Diretor da STI ou de um de seus Coordenadores.

**8.2** Após convocada, caberá à ETIR recomendar procedimentos a serem executados ou as medidas de recuperação a serem adotadas durante um incidente.

**8.3** Uma vez acatadas as recomendações e medidas, a ETIR poderá conduzir os tomadores de decisão a agir durante um incidente de segurança.

**8.4** Quando conveniente e necessário, o Diretor da STI autorizará a ETIR iniciar, por conta própria, o tratamento e resposta a determinadas classes de incidentes, devidamente caracterizadas e exemplificadas, seguidas dos limites de atuação, ou de comando para atuação, no processo de contorno, contenção ou solução dos respectivos incidentes classificados.

**8.5** A autorização a que se refere o item 8.4 se dará por meio de memorando circular aos Coordenadores da STI e ao Agente Responsável pela ETIR e deverá ser publicada no ambiente de disseminação do conhecimento da STI.

**8.6** A dedicação a atividades proativas, na forma do item 7.8, assim como a atuação por convocação, na forma do item 7.9, deverão ser acordadas entre o Agente Responsável e o respectivo supervisor de cada integrante envolvido.

## 9 SERVIÇOS

A ETIR prestará, inicialmente, o serviço reativo "Tratamento de Incidentes de Segurança em Redes Computacionais". Novos serviços poderão ser adicionados em futuras revisões deste normativo, a depender da necessidade

## 10 DISPOSIÇÕES GERAIS

**10.1** Norma que disciplina o Gerenciamento de Incidentes de Segurança da Informação versará, dentre outras diretrizes inerentes, sobre os serviços a serem prestados pela ETIR.

**10.2** Assim que possível, a implementação da ETIR deverá ser migrada para o modelo “2 - Centralizado”, conforme NC05, momento em que uma nova unidade da STI deverá ser criada, com chefia e quadro próprios, novas atribuições proativas e maior nível de autonomia.

**10.3** Este documento deverá ser revisado periodicamente, em intervalos de até dois anos.