PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO Nº 229/2013 (*)
REVOGADO PELO ATO DA PRESI N° 152/2018

~~Aprova a Norma Complementar de Criação da Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do Tribunal Regional do Trabalho da 7ª Região.~~

~~**A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO**, no uso de suas atribuições legais e regimentais,~~

~~**CONSIDERANDO** as boas práticas de Governança de TI que visam garantir a disponibilidade e integridade de sistemas, aplicativos, dados e de documentos digitais do TRT da 7ª Região;~~

~~**CONSIDERANDO** a necessidade de orientar a condução da Política de Segurança da Informação (PSI) em vigor no TRT da 7ª Região, visando garantir e incrementar a segurança da informação e das comunicações;~~

~~**CONSIDERANDO** a estratégia de segurança da informação composta por várias camadas, uma delas, que vem sendo adotada por diversas instituições, é a criação de equipes de tratamento e reposta a incidentes de segurança em redes de computadores,~~

~~**RESOLVE:**~~

~~**Art. 1º** Aprovar a Norma Complementar nº 03/NC/STI/SESTI, da Secretaria de Tecnologia da Informação, que dispõe sobre a criação da Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do Tribunal Regional do Trabalho da 7ª Região, na forma do anexo, para observância e aplicação em todo o Regional.~~

~~**Art. 2º** Este ato entra em vigor na data de sua publicação.~~

~~**PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.**~~
~~Fortaleza, 29 de maio de 2013.~~
~~**MARIA ROSELI MENDES ALENCAR**~~
~~Presidente~~

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1236, 31 mai. 2013.
Caderno Judiciário do Tribunal Regional do Trabalho da 7ª Região, p. 7.

ANEXO I

1 OBJETIVO

1.1 Disciplinar a criação de Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETRISRC) no âmbito do Tribunal Regional do Trabalho da 7ª Região.

2 CONSIDERAÇÕES INICIAIS

2.1 Nos últimos anos, o Tribunal Regional do Trabalho da 7ª Região vem implementando e consolidando a sua rede local de computadores cada vez mais ampla, como exigência para suportar o fluxo crescente de informações, bem como permitir que seus usuários acessem à rede mundial de computadores para melhor desempenharem suas funções. Manter a segurança da informação e comunicações de uma organização em um ambiente computacional interconectado nos dias atuais é um grande desafio, que se torna mais difícil à medida que são lançados novos produtos para a *Internet* e novas ferramentas de ataque são desenvolvidas.

2.2 Diante da premissa de garantir e incrementar a segurança da informação e comunicações no Tribunal Regional do Trabalho da 7ª Região, há a necessidade de orientar a condução da Política de Segurança Institucional (PSI) em vigor.

2.3 Considerando a estratégia de segurança da informação composta por várias camadas, uma delas, que vem sendo adotada por diversas instituições, é a criação de Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais, mundialmente conhecido como CSIRT® (do inglês "Computer Security Incident Response Team").

2.4 É competência do Setor de Escritório de Segurança de TI da Secretaria de Tecnologia da Informação, apoiar o Tribunal Regional do Trabalho da 7ª Região, nas atividades de capacitação e tratamento de incidentes de segurança em sua rede de computadores.

3 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

3.1 Item IV, Art. 6º da Lei nº 10.683, de 28 de maio de 2003, que dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências.

3.2 Decreto nº 3.505, de 13 de junho de 2000, que Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

3.3 Art. 10 da Resolução nº 90, de 29 de setembro de 2009, do Conselho Nacional de Justiça, estabelece que "a estrutura organizacional, o quadro de pessoal, a gestão de ativos e os processos do setor responsável pela gestão de trabalho da área de TIC do Tribunal deverão estar adequados às melhores práticas preconizadas pelos padrões nacionais e internacionais para as áreas de governança e de gerenciamento de serviços de TIC".

3.4 Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008, "compete ao Departamento de Segurança da Informação e Comunicações estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta".

3.5 Norma Complementar 05/IN01/DSI/GSIPR, do Departamento de Segurança da Informação e Comunicações, do Gabinete de Segurança Institucional, da PRESIDÊNCIA DA REPÚBLICA, que normatiza a Criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais (ETIR).

3.6 ABNT NBR ISO/IEC 27002:2005 - Código de prática para a gestão da segurança da informação.

4 CONCEITOS E DEFINIÇÕES

4.1 Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

a) agente responsável: Servidor Público ocupante de cargo efetivo carreira do Tribunal Regional do Trabalho da 7ª região incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
b) comunidade ou Público Alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais;
c) 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 – Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República – GSI;
d) equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETRISRC): Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;
e) incidente de segurança: evento adverso, confirmado ou sob suspeita, relacionado à informação ou dos sistemas de computação ou das redes de computadores;
f) serviço: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais;
g) 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;
h) vulnerabilidade: é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

5 RESPONSABILIDADE

5.1 O Setor de Escritório de Segurança de Tecnologia da Informação é o responsável por coordenar a instituição, implementação e manutenção da infraestrutura necessária a Equipe de Tratamento e Resposta a Incidentes de segurança na rede de computadores do Tribunal Regional do Trabalho da 7ª Região.

5.2 Ao Agente Responsável, caberá criar os procedimentos internos, gerenciar as atividades e distribuir tarefas para a Equipe ou Equipes que compõem a ETRISRC e de ser a interface com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR GOV).

6 DEFINIÇÃO DA MISSÃO

6.1 Garantir o cumprimento da missão institucional do Tribunal Regional do Trabalho da 7ª Região através da solução dos incidentes de segurança na rede interna de computadores.

7 MODELO DE IMPLEMENTAÇÃO

7.1 O modelo a ser utilizado pelo Tribunal Regional do Trabalho a 7ª Região é o que utiliza a própria equipe de Tecnologia da Informação (TI).

7.2 Não existirá um grupo dedicado exclusivamente às funções de tratamento e resposta a incidentes de segurança em rede. A Equipe será formada a partir dos membros das equipes da Secretaria de Tecnologia da Informação do Tribunal Regional do Trabalho da 7ª Região, que além de suas funções regulares passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes de segurança na rede de computadores interna do Tribunal Regional do Trabalho da 7ª Região.

7.3 Neste modelo as funções e serviços de tratamento de incidentes de segurança deverão ser realizadas, preferencialmente, por administradores de rede ou de sistemas ou, ainda, por peritos em segurança.

7.4 A Equipe desempenhará suas atividades, via de regra, de forma reativa, sendo desejável, porém que o Agente Responsável pela ETRISRC atribua responsabilidades para que os seus membros exerçam atividades pró-ativas.

8 ESTRUTURA ORGANIZACIONAL

8.1 A ETRISRC ficará subordinada à Setor de Escritório de Segurança de TI, da Secretaria de Tecnologia da Informação do Tribunal Regional do Trabalho da 7ª Região.

8.2 Compete ao Setor de Escritório de Segurança de TI coordenar a Equipe de Tratamento de Incidentes de segurança em Redes Computacionais do Tribunal Regional do Trabalho da 7ª Região.

8.3 Atribuições do Gestor da ETRISRC:

a) coordenar a instituição, implementação e manutenção da infraestrutura necessária à ETRISRC;
b) garantir que os incidentes de segurança na Rede de Computadores do Tribunal Regional do Trabalho da 7ª Região sejam monitorados;
c) adotar procedimentos de *feedback* para assegurar que os usuários que comuniquem incidentes de segurança da informação e comunicações na rede interna de computadores sejam informados dos procedimentos adotados;
d) apoiar os treinamentos relacionados à Segurança da Informação e Comunicações fornecendo casos práticos de incidentes de segurança na rede interna de computadores, garantindo-se a confidencialidade e devidos níveis de sigilo, sobre o que poderia acontecer, como reagir a tais incidentes e como evitá-los no futuro.

8.4 É de competência da ETRISRC:

a) recolher provas o quanto antes após a ocorrência de um incidente de Segurança da Informação e Comunicações na rede interna de computadores;
b) executar uma análise crítica sobre os registros de falhas para assegurar que elas foram satisfatoriamente resolvidas;
c) investigar as causas dos incidentes de Segurança da Informação e Comunicações na rede interna de computadores;

d) implementar mecanismos para permitir a quantificação e monitoração dos tipos, volumes e custos de incidentes e falhas de funcionamento;
e) indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes.

8.5 A ETRISRC será composta por:
a) 1 Servidor do SATI (Setor de Ambiente de TI);
b) 1 Servidor do SGAS (Setor de Garantia de Serviços);
c) 1 Servidor do SSUPN3 (Setor de Suporte Nível 3).

8.6 Caso necessário, poderão ser convocados para comporem a ETIR:
a) 1 Servidor da AJA (Assessoria Jurídica Administrativa);
b) 1 Servidor da Secretaria de Gestão de Pessoas;
c) 1 Servidor da Assessoria de Comunicação Social.

8.7 Para cada uma das posições deverá ser designado 1 suplente que deverá ter condições de substituir o titular e executar todas as suas atribuições como se o mesmo fosse.
8.8 O Diretor da Secretaria de Tecnologia da Informação através de Portaria indicará os servidores para as funções relacionadas acima e seus respectivos suplentes.

9 AUTONOMIA DA ETRISRC

9.1 A equipe da ETRISRC tem plena autonomia para tomada de decisão sobre quais medidas serão adotadas e poderá conduzir o público alvo para realizar ações ou as medidas necessárias para reforçar a resposta ou a postura da organização na recuperação de incidentes de segurança na rede interna de computadores. Durante um incidente de segurança, se justificável, a equipe poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

10 DISPOSIÇÕES GERAIS

10.1 O Tribunal Regional do Trabalho da 7ª Região que inicialmente optou pela implantação do Modelo de Implementação, utilizando a equipe de Tecnologia da Informação, deverá, assim que possível, migrar para um dos outros modelos, Centralizado, Descentralizado ou Misto, conforme a Norma Complementar 05/IN01/D Segurança da Informação e Comunicações/GSIPR de 14 de agosto de 2009.
10.2 A Equipe deve ser composta por servidores públicos ocupantes de cargo efetivo de carreira, com perfil técnico compatível.
10.3 A ETRISRC deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de segurança em rede orientados pelo Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR GOV).
10.4 A ETRISRC poderá usar as melhores práticas de mercado, desde que não conflitem com os dispositivos desta Norma Complementar.
10.5 A ETRISRC deverá comunicar de imediato a ocorrência de todos os incidentes de segurança ocorridos na sua área de atuação ao CTIR GOV, conforme padrão definido por esse Órgão, a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal.

11 VIGÊNCIA

11.1 Esta Norma Complementar entra em vigor na data de sua publicação.

ANEXO II

DOCUMENTO DE CONSTITUIÇÃO DA ETRISRC

O Tribunal Regional do Trabalho da 7ª Região, alinhado com a sua Política de Segurança Institucional, constitui a Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETRISRC), ficando o seu funcionamento regulamentado na forma abaixo.

1 MISSÃO

Garantir o cumprimento da missão institucional do Tribunal Regional do Trabalho da 7ª Região através da solução dos incidentes de segurança na rede interna de computadores.

2 COMUNIDADE OU PÚBLICO ALVO

A ETRISRC atenderá internamente a seguinte comunidade, composta por: Magistrados, servidores ocupantes de cargo efetivo ou cargo em comissão, requisitados e cedidos, funcionários de empresas prestadoras de serviços terceirizados, consultores, estagiários, pensionistas, bem como Magistrados e servidores inativos.

E externamente o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR GOV) e outros órgãos da Administração Pública Federal que atuam no mesmo campo da ETRISRC do Tribunal Regional do Trabalho da 7ª Região, fornecendo informações a cerca dos incidentes de segurança ocorridos na rede do Tribunal Regional do Trabalho da 7ª Região, alimentando as suas bases de conhecimentos e fomentando a troca de tecnologias.

A comunicação do tratamento dos incidentes de segurança para a comunidade interna e externa será efetuada através dos canais de comunicação oficiais do Tribunal Regional do Trabalho da 7ª Região.

3 MODELO DE IMPLEMENTAÇÃO

O modelo utilizado pela ETRISRC será misto e será composto por uma Equipe de Tratamento e Resposta a Incidentes de segurança em Redes Computacionais.

A Equipe será a responsável por criar as estratégias, gerenciar as atividades, além de ser a responsável, perante toda a organização, pela comunicação com o CTIR GOV.

4 ESTRUTURA ORGANIZACIONAL

4.1 A ETRISRC ficará subordinada à Setor de Escritório de Segurança de TI, da Secretaria de Tecnologia da Informação do Tribunal Regional do Trabalho da 7ª Região.

4.2 Compete ao Setor de Escritório de Segurança de TI coordenar a Equipe de Tratamento de Incidentes de segurança em Redes Computacionais Tribunal Regional do Trabalho da 7ª Região atribuições do Gestor da ETRISRC:

a) coordenar a instituição, implementação e manutenção da infraestrutura necessária à ETIR;

b) garantir que os incidentes de segurança em Redes Computacionais da Rede de Computadores do Tribunal Regional do Trabalho da 7ª Região sejam monitorados;
c) adotar procedimentos de *feedback* para assegurar que os usuários que comuniquem incidentes de segurança da informação e comunicações sejam informados dos procedimentos adotados;
d) apoiar os treinamentos relacionados à Segurança da Informação e Comunicações fornecendo casos práticos de incidentes de segurança, garantindo-se a confidencialidade e devidos níveis de sigilo, sobre o que poderia acontecer, como reagir a tais incidentes e como evitá-los no futuro.

4.3 É de competência da ETRISRC:
a) recolher provas o quanto antes após a ocorrência de um incidente de Segurança da Informação e Comunicações;
b) executar uma análise crítica sobre os registros de falha para assegurar que as mesmas foram satisfatoriamente resolvidas;
c) investigar as causas dos incidentes de Segurança da Informação e Comunicações;
d) implementar mecanismos para permitir a quantificação e monitoração dos tipos, volumes e custos de incidentes e falhas de funcionamento;
e) indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes de segurança.

4.4 A ETRISRC será composta por:
a) servidor do SATI (Setor de Ambiente de TI);
b) servidor do SGAS (Setor de Garantia de Serviços);
c) servidor do SSUPN3 (Setor de Suporte Nível 3).

4.5 Caso necessário, poderão ser convocados para comporem a ETRISRC:
a) servidor da AJA (Assessoria Jurídica Administrativa);
b) servidor da Secretaria de Gestão de Pessoas;
c) servidor da Assessoria de Comunicação Social.

Para cada uma das posições deverá ser designado 1 suplente que deverá ter condições de substituir o titular e executar todas as suas atribuições como se o mesmo fosse.
O Diretor da Secretaria de tecnologia da Informação através de Portaria indicará os servidores para as funções relacionadas acima e seus respectivos suplentes.

5 AUTONOMIA DA ETRISRC

A autonomia da ETRISRC será completa no processo de tomada de decisão sobre quais medidas serão adotadas e poderá conduzir o público alvo para realizar ações ou as medidas necessárias para reforçar a resposta ou a postura da organização na recuperação de incidentes de segurança. Durante um incidente de segurança, se tal se justificar, a Equipe poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

6 SERVIÇOS

São serviços da ETRISRC:
a) implementar, no mínimo, o Tratamento de Incidentes de Segurança em Redes computacionais, contemplando o tratamento de artefatos maliciosos;
b) tratamento de vulnerabilidades;

c) ~~emissão de alertas e advertências;~~
d) ~~prospecção e monitoração de novas tecnologias;~~
e) ~~avaliação de segurança;~~
f) ~~detecção de intrusão;~~
g) ~~disseminação de informações relacionadas a segurança.~~

(*) Revogado pelo Ato da Presidência n° 152/2018 Disponibilizado no Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2571, 28 set. 2018. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 1.