PODER JUDICIÁRIO
TRIBUNAL REGIONAL DO TRABALHO DA 8ª REGIÃO

PORTARIA PRESI N° 248, DE 21 DE MARÇO DE 2018

Institui o Processo de Gerenciamento de Incidentes de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 8ª Região.

A DESEMBARGADORA VICE-PRESIDENTE, NO EXERCÍCIO DA PRESIDÊNCIA, DO TRIBUNAL REGIONAL DO TRABALHO DA OITAVA REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO as ações previstas no Planejamento Estratégico de Tecnologia da Informação e Comunicação do Tribunal Regional do Trabalho da 8ª Região com a implantação dos controles da ISO 27001 aderentes à Política de Segurança da Informação do TRT da 8ª Região;

CONSIDERANDO a observância das recomendações do Código de Boas Práticas em Segurança da Informação publicado pelo Tribunal de Contas da União;

CONSIDERANDO a Instrução Normativa n° 8, do Gabinete de Segurança Institucional da Presidência da República, de 19 de agosto de 2010, que estabelece diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da Administração Pública Federal;

RESOLVE:

Art. 1° Instituir o Processo de Gerenciamento de Incidentes de Segurança da Informação no âmbito do Tribunal Regional Trabalho da Oitava Região.

CAPÍTULO I
DOS CONCEITOS E DEFINIÇÕES

Art. 2° Para os efeitos desta Portaria são estabelecidos os seguintes conceitos e definições:

I. Ações maliciosas: é a ação provocada por 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;

II. Central de Serviços de TIC: ponto único de contato entre o provedor de serviço de TIC e os usuários, responsável pela gerência de incidentes, de requisições de serviços e também pela comunicação com os usuários;

III. Incidente de Segurança da Informação: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, que comprometa a confidencialidade, integridade e/ou a disponibilidade dos sistemas;

IV. Plano de Continuidade dos Serviços Essenciais de TIC: documentação dos procedimentos e informações necessárias para que o Tribunal mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido em casos de incidentes;

V. Provedor de Serviços de TIC: unidade organizacional ou pessoa que oferece Serviços de TIC para usuários internos ou externos;

VI. Sistema de Gerenciamento de Serviços de TIC: software adotado pelo Tribunal, tornando-se, a partir de então, de uso obrigatório para registro de incidentes ou requisições de serviços de TIC;

VII. Tratamento de Incidentes de Segurança da Informação: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança da informação, procurando extrair informações que permitam impedir a continuidade da ação maliciosa;

VIII. Vulnerabilidade: é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a

exploração maliciosa e acessos indesejáveis ou não autorizados.

CAPÍTULO II
DO PROCESSO

Art. 3° O Processo de Gerenciamento de Incidentes de Segurança da Informação tem como objetivo principal restaurar a operação normal do serviço o mais breve possível, minimizando o impacto adverso nas operações de negócio ocasionado pelo incidente de segurança.

Art. 4° As regras gerais do Processo de Gerenciamento de Incidentes de Segurança da Informação consideram que:

I. Todos os incidentes notificados ou detectados devem ser registrados, controlados, tratados e gerenciados por meio do Sistema de gerenciamento de Serviços de TIC, adotado e formalizado pelo Tribunal;
II. O registro dos incidentes poderá ser realizado por telefone, e-mail ou com a utilização de ferramenta de gerenciamento de serviços de TIC adotada no Tribunal;

CAPÍTULO III
DOS PAPÉIS E RESPONSABILIDADES

Art. 5° O Processo de Gerenciamento de Incidentes de Segurança da Informação será gerenciado pelo Assistente de Segurança da Informação.

Art. 6° Para a execução do processo de cumprimento de requisição, são estabelecidos os seguintes papeis e responsabilidades:

I. Analista da Central de Serviços de TIC: atua como ponto único de contato entre os usuários e a área de TI, recebendo e registrando ocorrências ou suspeitas de incidentes de Segurança da Informação.

II. Grupo Solucionador: responsável por resolver as ocorrências e manter a Central de Serviços informada sobre o andamento dos incidentes de Segurança da Informação. No escopo dos serviços de segurança da informação inclui-se:

a) Tratamento de artefatos maliciosos: Este serviço prevê o recebimento de informações ou cópia do artefato malicioso que foi utilizado no ataque, ou em qualquer outra atividade desautorizada ou maliciosa. Uma vez recebido o artefato o mesmo deve ser analisado para que seja sugerida uma estratégia de detecção, remoção e defesa contra este artefato;

b) Tratamento de vulnerabilidades: Este serviço prevê o recebimento de informações sobre vulnerabilidades, quer sejam em hardware ou software, objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção dessas vulnerabilidades;

c) Emissão de alertas de segurança da informação: Este serviço consiste em divulgar alertas ou advertências imediatas como uma reação diante de um incidente de segurança em redes de computadores ocorrido, com o objetivo de advertir os usuários ou dar orientações sobre como devem agir diante do problema;

d) Anúncios: Este serviço consiste em divulgar, de forma proativa, alertas sobre vulnerabilidades e problemas de incidentes de segurança em redes de computadores em geral, cujos impactos sejam de médio e longo prazo, possibilitando que os usuários se preparem contra novas ameaças;

e) Detecção de intrusão: Este serviço prevê a análise do histórico de dispositivos que detectam as tentativas de intrusões em redes de computadores, com vistas a identificar e iniciar os procedimentos de resposta a incidente de segurança em redes de computadores, com base em eventos com características pré-definidas, que possam levar a uma possível intrusão;

f) Disponibilização dos Sistemas: Este serviço tem por objetivo manter disponíveis os sistemas do Tribunal pelo máximo de tempo possível. Diante de um incidente de segurança da informação que cause interrupção dos

sistemas do Tribunal, o Plano de Continuidade dos Serviços Essenciais de TIC poderá ser acionado até que o sistema seja restabelecido à sua normalidade.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 7° O desenho do Processo de Gerenciamento de Incidentes de Segurança com suas entradas, atividades relacionadas e saídas, ficarão disponíveis no sítio da intranet deste Tribunal.

Parágrafo único. A atualização do Processo de Gerenciamento de Incidentes de Segurança ficará a cargo da SETIN, que deverá revisá-lo periodicamente.

Art. 8° Os casos omissos e emergenciais serão resolvidos pelo Comitê Gestor de Segurança da Informação.

Art. 9° Esta Portaria entra em vigor na data de sua publicação.

Publique-se, dê-se ciência e cumpra-se.

SULAMIR PALMEIRA MONASSA DE ALMEIDA
Desembargadora Vice-Presidente
no exercício da Presidência