Estado do Ceará
Poder Judiciário
Tribunal de Justiça
Comitê Gestor de Segurança da Informação
Anexo IV

PJSETIN2015004 – Implantação do Programa de Segurança Corporativa da Informação no âmbito do Poder Judiciário do Estado do Ceará

04/NSI04/CGSI/TJCE – **Norma para Tratamento de códigos Maliciosos**

Sumário

1 **Objetivo**

1.1 Definir as diretrizes relacionadas as ações contra códigos maliciosos no âmbito do Poder Judiciário Estadual Cearense.

2 **Abrangência**

2.1 Esta norma abrange todos os usuários que utilizam os **sistemas de informações, equipamentos, serviços e banco de dados** no ambiente de Tecnologia da Informação do Poder Judiciário do Estado do Ceará.

3 **Termos e Definições**

3.1 Usuário: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, conveniados, consultores, estagiários, e demais pessoas que se encontrem a serviço do Poder Judiciário do Estado do Ceará, utilizando em caráter temporário os recursos tecnológicos deste Poder.

3.2 Código Malicioso ou *Malware*: termo genérico que se refere a todos os tipos de programa especificamente desenvolvidos para executar ações danosas em recursos de Tecnologia da Informação, tais como vírus, cavalo de tróia, *spyware, worms, bots, backdoors, keyloggers, rootkits, bots, botnets etc*.

3.3 Vírus: é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador.

3.4 Cavalo de Tróia: e um programa, normalmente recebido como um “presente” (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

3.5 Spyware: é o termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros.

3.6 Backdoors: programas que permitem o retorno de um invasor a um computador comprometido, utilizando serviços criados ou modificados para este fim.

3.7 Keyloggers: é um programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador.

3.8 Worms: é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador.

3.9 Bots: é um programa capaz de propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador.

3.10 Botnets: são redes formadas por computadores infectados com bots.

3.11 Rootkits: Conjunto de programas que fornece mecanismos utilizados por invasores para esconder e assegurar a sua presença no computador comprometido.

3.12 Log: arquivo que contém informações sobre eventos de qualquer natureza em um sistema computacional, análise forense para a elucidação de incidentes de segurança, auditoria de processos, cumprimento de exigências legais para a manutenção de registro do histórico de acessos ou eventos e para a resolução de problemas.

4 **Diretrizes**

4.1 Os recursos de Tecnologia da Informação devem estar providos de sistemas de detecção e bloqueio de códigos maliciosos, prevenção e detecção de acesso não autorizado.

4.2 Havendo correções ou atualizações para os sistemas de detecção e bloqueio de códigos maliciosos, as mesmas devem ser implementadas, a fim de se evitar que os sistemas de informações e o parque tecnológico fiquem vulneráveis a códigos maliciosos ou a qualquer tentativa de acesso não autorizado.

4.3 Mídias que são utilizadas nos equipamentos computacionais devem ser verificadas automaticamente, quanto à contaminação por código malicioso, antes de sua utilização.

4.4 Os sistemas de detecção e bloqueio de códigos maliciosos devem prover monitoramento, em tempo de execução, dos arquivos e programas, quanto à contaminação por código malicioso.

4.5 Padrões e procedimentos para instalação, configuração, utilização e atualização de sistemas de detecção e bloqueio de códigos maliciosos devem ser estabelecidos pela área de

tecnologia da Informação.

4.6 O usuário, em caso de evidência da ação de código malicioso ou problemas na funcionalidade do antimalware, deverá registrar chamado na Central de Atendimento de Tecnologia da Informação (Cati).

5 **Competências e Responsabilidades**

5.1 **Dos Usuários/Colaboradores e dos em Regime de Exceção (Temporários)**

5.1.1 Não interromper o escaneamento programado do antimalware.

5.1.2 Comunicar à Cati todas as anormalidades detectadas nos sistemas e computadores sob sua responsabilidade.

5.2 **Dos Custodiantes da Informação**

5.2.1 **Da Área de Tecnologia da Informação**

5.2.1.1 Auxiliar no processo de conscientização dos usuários quanto às melhores práticas de prevenção contra códigos maliciosos.

5.2.1.2 Garantir a instalação dos sistemas de detecção e bloqueio de programas maliciosos nos equipamentos computacionais, mantendo-os atualizados, conforme disponibilização do fabricante.

5.2.1.3 Monitorar os logs dos sistemas de detecção e bloqueio de códigos maliciosos, prevenção e detecção de acesso não autorizado, com objetivo de atuar de forma proativa na identificação de ameaças.

5.2.2 **Do Serviço de Segurança da Informação**

5.2.2.1 Promover divulgação das regras presentes neste documento, acompanhar as auditorias dos sistemas e reportar ao Comitê Gestor de Segurança da Informação as ameaças à Política de Segurança da Informação.

5.2.2.2 Auxiliar no processo de conscientização dos usuários quanto às melhores práticas de prevenção contra códigos maliciosos.

5.2.3 **Do Comitê Gestor de Segurança da Informação**

5.2.3.1 O comitê será acionado quando a área de Segurança da Informação julgar

pertinente.

5.3 **Do Monitoramento e da Auditoria do Ambiente**

5.3.1 A auditoria será promovida pela respectiva área de tecnologia da informação, verificando a adoção das regras contidas no presente documento. Periodicamente, a pedido do Serviço de Segurança da Informação, a área de tecnologia da informação remeterá relatórios.

6 **Penalidades**

6.1 No caso de evidências de uso irregular do uso do Antimalware (antivirus), o usuário terá seu acesso ao computador bloqueado para averiguação.

6.2 O usuário infrator deverá ser notificado e a ocorrência de transgressão comunicada ao seu chefe imediato e à diretoria correspondente.

6.3 O acesso somente será restabelecido mediante solicitação da chefia imediata, informando que tomou conhecimento da violação das normas de segurança.

6.4 O Comitê Gestor de Segurança da Informação será informado e tomará as medidas que julgar necessárias.

6.5 As penalidades poderão incluir: bloqueio temporário, cancelamento dos acessos, processos administrativos, criminais e cíveis, além da aplicação das penalidades previstas em lei.

7 **Vigência**

7.1 Esta Norma entra em vigor na data de sua publicação.