NSI 011 - PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

1. OBJETIVO

Dispor sobre as regras de segurança que nortearão a definição e a implantação de medidas para a proteção contra a ação de códigos maliciosos no ambiente de rede do Tribunal Regional Eleitoral da Bahia.

2. CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

Antivírus: ferramenta desenvolvida para detectar, anular e eliminar vírus e outros tipos de códigos maliciosos de um computador. Pode incluir também a funcionalidade de *firewall* pessoal;

Código malicioso: termo genérico que se refere a todos os tipos de programas especificamente desenvolvidos para executar ações danosas em recursos de tecnologia da informação;

Firewall: dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores;

***Firewall* pessoal**: tipo específico de *firewall*. Programa usado para proteger um computador contra acessos não autorizados; e

Log: registro de atividades gerado por programas e serviços de um computador. Termo técnico que se refere ao registro de atividades de diversos tipos como, por exemplo: de conexão (informações sobre a conexão de um computador à Internet) e de acesso a aplicações (informações de acesso de um computador a uma aplicação de Internet).

3. CONSIDERAÇÕES INICIAIS

Conforme estabelecido na **NSI-002 – Uso de Recursos de Tecnologia da Informação e Controle de Acesso**, os usuários são responsáveis pelos recursos de tecnologia da informação por eles utilizados, devendo contribuir para seu funcionamento e segurança.

Códigos maliciosos são agentes potencialmente graves à segurança da informação, pois possibilitam o roubo de informações sigilosas e a paralisação dos serviços.

Convém que os recursos de tecnologia da informação estejam protegidos por sistemas de detecção e bloqueio de códigos maliciosos, prevenção e detecção de acesso não autorizado, tais como programas antivírus, programas de análise de conteúdo de correio eletrônico e *firewall*.

Padrões e procedimentos para instalação, configuração, utilização e atualização de sistemas de detecção e bloqueio de códigos maliciosos devem ser estabelecidos pela Secretaria de Tecnologia da Informação.

4. CONTROLES

É vedada qualquer atividade, por parte dos usuários, que vise à criação ou distribuição de códigos maliciosos.

É vedada ao usuário a desativação ou a alteração de configuração de quaisquer de seus componentes de proteção contra códigos maliciosos (por ex.: antivírus, *firewall* pessoal etc.). Caso julgue necessário alguma modificação, o setor responsável deverá ser informado.

Antes de sua utilização, é conveniente que toda e qualquer mídia de armazenamento que tenha origem externa ao Tribunal seja verificada quanto à existência de códigos maliciosos.

Convém que todo e qualquer arquivo recebido por correio eletrônico ou Internet seja verificado de forma automática quanto à existência de códigos maliciosos.

Convém que todos os dispositivos de processamento do Tribunal devam estar configurados de acordo com os padrões de segurança mais adequados aos serviços previstos, de maneira que prestem apenas os serviços previstos.

Convém que todos os dispositivos de processamento do Tribunal estejam atualizados conforme as recomendações dos respectivos fabricantes e fornecedores.

Os dispositivos de processamento portáteis, sempre que tecnicamente possível, devem possuir *firewall* pessoal instalado e configurado de forma a possibilitar que o dispositivo seja utilizado somente para os fins previstos.

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.

Os arquivos contaminados por código malicioso devem ser imediatamente descontaminados, isolados ou removidos do sistema pelo programa antivírus. Em caso de persistência do problema, o equipamento deve ser isolado até que seja sanado o problema para não afetar o desempenho das atividades do Tribunal.

5. COMPETÊNCIAS E RESPONSABILIDADES

Ficam definidas as seguintes competências e responsabilidades:

À Secretaria de Tecnologia da Informação:

1. auxiliar a Comissão de Segurança da Informação no processo de conscientização dos usuários quanto às melhores práticas de prevenção contra códigos maliciosos;
2. proceder com a instalação dos sistemas de detecção e bloqueio de códigos maliciosos nos equipamentos computacionais, mantendo-os atualizados conforme disponibilização do fabricante; e.

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.

Ao usuário:

1. utilizar somente programas homologados pela Secretaria de Tecnologia da Informação;
2. observar se o programa de antivírus está instalado e ativo no equipamento computacional;
3. utilizar mídia de armazenamento que tenha origem externa à organização conforme disposto no item 4.3; e
4. notificar imediatamente à Comissão de Segurança da Informação e/ou Secretaria de Tecnologia da Informação qualquer suspeita de ataque por código malicioso à dispositivo de processamento sob sua custódia, ou mesmo a sua rede local.

6. DISPOSIÇÕES FINAIS

As atualizações e as correções para os sistemas de detecção e bloqueio de códigos maliciosos devem ser homologadas pela Secretaria de Tecnologia da Informação antes de aplicadas ao ambiente de produção.

As correções ou atualizações para os sistemas de detecção e bloqueio de códigos maliciosos, depois de homologadas, devem ser implementadas, a fim de se evitar que estes sistemas fiquem vulneráveis a códigos maliciosos ou a qualquer tentativa de acesso não autorizado.

Os casos omissos e as dúvidas surgidas na aplicação desta norma serão dirimidos pelo Comitê Gestor de Segurança da Informação.

7. VIGÊNCIA E ATUALIZAÇÃO

A atualização desta norma ocorrerá de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de 02 (dois) anos.