ANEXO X
NORMA DE PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo

Versionamento:

Versão:	1.0
Data:	03/04/2023
Criada por:	Grupo de Trabalho Técnico SGSI - DIA
Aprovada por:	Comitê de Governança de Segurança da Informação
Aprovada em:	12/06/2023

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações

1. INTRODUÇÃO

A norma de proteção contra códigos maliciosos complementa a Política de Segurança da Informação (PSI), definindo as diretrizes para proteção dos ativos e/ou recursos de Tecnologia da Informação e Comunicação (TIC) do Poder Judiciário do Estado do Maranhão (PJMA) contra códigos maliciosos de qualquer natureza.

Para fins desta norma, aplica-se a lista de termos do glossário com suas respectivas definições, conforme descrito no ANEXO I da PSI.

Esta norma obedece ao escopo definido na Política de Segurança da Informação.

2. OBJETIVO

Assegurar que informações, ativos de TIC e recursos de processamento da informação estejam protegidos contra códigos maliciosos.

3. DIRETRIZES

Orientações da norma de proteção contra códigos maliciosos.

3.1 Ferramenta de proteção contra códigos maliciosos

O Poder Judiciário do Estado do Maranhão disponibilizará nos seus ativos de TIC uma ferramenta de proteção contra códigos maliciosos. A ferramenta deverá realizar a proteção contra diversos tipos de malwares, tais como: vírus, ransomware, cavalo de tróia (trojan), backdoor, verme (worm), Remote Access Trojan - RAT, spyware (screenlogger, keylogger e adware), rootkit e similares, devendo ser instalada nos seguintes ativos de TIC:

I - computadores de mesa (desktop);

II - dispositivos móveis corporativos (notebooks, celulares, smartphones e tablets);

III - servidores de rede (arquivos, aplicações, etc.).

A ferramenta de proteção contra códigos maliciosos do Poder Judiciário do Estado do Maranhão adotará as seguintes regras de uso:

I - atualização diária, em tempo real, do arquivo de assinaturas de códigos maliciosos;

II - realização de verificações automáticas, agendadas e manuais conforme a necessidade nos ativos de TIC suportados (computadores de mesa, dispositivos móveis corporativos e servidores de rede) do PJMA;

III - as verificações automáticas deverão analisar todos os arquivos em cada uma das unidades de armazenamento locais, inclusive as originadas a partir de dispositivos de armazenamento removíveis (mídias de CD's, DVD's e/ou BLU-RAY, pendrives e discos rígidos externos), conectados aos computadores de mesa e dispositivos móveis corporativos;

IV - as verificações automáticas nos servidores de rede serão limitadas a pastas ou arquivos específicos, previamente definidas pela DIA, de modo a evitar o comprometimento do desempenho do seus recursos computacionais (alto consumo do uso de CPU, memória, disco rígido, etc.);

V - as funções de proteção em tempo real e detecção com base no comportamento da ameaça, deverão estar habilitadas para todos os ativos de TIC suportados;

VI - sítios eletrônicos, serviços e arquivos acessados, baixados ou executados da internet, bem como softwares não autorizados ou não licenciados detectados serão automaticamente bloqueados nos ativos de TIC suportados.

Caso um servidor de rede esteja infectado ou com suspeita de infecção de código malicioso, serão adotadas medidas para garantir o isolamento do mesmo da rede corporativa e da internet, levando em consideração o impacto da desativação dos serviços publicados no referido servidor, bem como preservar as informações necessárias para posterior auditoria.

3.2 Prevenção dos(as) usuários(as) contra códigos maliciosos

Mesmo com a presença da ferramenta para proteção contra códigos maliciosos nos ativos de TIC do PJMA, os(as) usuários(as) deverão adotar um comportamento cauteloso, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos.

Os(As) usuários(as) deverão notificar imediatamente a DIA, utilizando os canais oficiais de comunicação ou solicitação do PJMA, de qualquer infecção ou

suspeita de infecção por código malicioso nos ativos de TIC suportados que tomem ciência.

É vedado aos(às) usuários(as):

I - instalar outra ferramenta de proteção contra códigos maliciosos de ativos de TIC que não seja a disponibilizada pelo PJMA;

II - remover/desinstalar ou desativar a ferramenta oficial de proteção contra códigos maliciosos de ativos de TIC do PJMA;

III - tentar efetuar o tratamento e correção de códigos maliciosos por iniciativa própria;

IV - desenvolver, testar ou armazenar partes de códigos de qualquer tipo, a menos que expressamente autorizado;

V - impedir, através de qualquer meio, a verificação automática da ferramenta de proteção contra códigos maliciosos, principalmente ao fazer uso dos dispositivos de armazenamento removíveis;

VI - habilitar MACROS para arquivos provenientes de fontes suspeitas, baixados ou recebidos da internet. Caso necessário, deverá ser solicitado o apoio da DIA para validar se o arquivo representa ou não uma ameaça.

4. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

4.1 Diretoria de Informática e Automação

Compete à Diretoria de Informática e Automação:

I - instalar e gerir a ferramenta de proteção e controle contra códigos maliciosos nos ativos de TIC suportados;

II - tratar os casos de infecção ou suspeita de infecção por códigos maliciosos;

III - garantir que novas modalidades de códigos maliciosos sejam adequadamente investigadas e tratadas e os ativos de TIC protegidos pela ferramenta adotada pelo PJMA;

IV - garantir a divulgação, por meio de treinamentos e informativos periódicos, de informações de ameaças, códigos maliciosos e medidas de proteção para os(as) usuários(as) do PJMA.

5. INFRAÇÕES E PENALIDADES

Infrações e penalidades serão aplicadas conforme previsto na Política de Segurança da Informação.

6. REVISÕES

Esta norma será alterada mediante necessidade de atualização, com apreciação e aprovação do Comitê de Governança de Segurança da Informação (CGSI).

7. APROVAÇÃO

A norma foi aprovada pelo Comitê de Governança de Segurança da Informação (CGSI), revogando-se todas as disposições em contrário.