POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

DA PROCURADORIA-GERAL DO ESTADO DO CEARÁ

NR08 - Combate a Softwares Maliciosos

Setembro/2022

CEARÁ
GOVERNO DO ESTADO
PROCURADORIA-GERAL DO ESTADO

CONTROLE DE VERSÕES

Versão	Data	Responsável	Alteração principal
00	07/11/2022	Coordenadoria de TI	Elaboração inicial

SUMÁRIO

1. INTRODUÇÃO

Entende-se por Softwares Maliciosos, todo aplicativo de computação que tenha o objetivo de causar danos, comprometendo a segurança em seus pilares (confiabilidade, disponibilidade e integridade). Para mitigar estas ameaças, existem controles e recursos de proteção como: antivírus, antispam, firewall pessoal, anti-spyware que podem ser utilizados a fim de assegurar a proteção necessária aos recursos de TIC da PGE-CE.

2. OBJETIVO

Definir as medidas preventivas de proteção, detecção e correção para resguardar o ambiente de TIC da PGE-CE contra softwares maliciosos.

3. ABRANGÊNCIA

Estes controles se aplicam a todos os usuários internos, que utilizam os recursos de TIC da PGE-CE.

4. COMBATE A SOFTWARES MALICIOSOS

4.1. Para aperfeiçoamento do controle e gerenciamento das políticas de segurança de informação, deve ser preferencialmente adotado o uso do Sistema Operacional Windows;

4.2. Todos os equipamentos com o Sistema Operacional Windows e servidores de rede que façam uso do compartilhamento de arquivos através da rede deverão estar protegidos com sistemas de proteção contra softwares maliciosos;

4.3. Não é permitido que o usuário remova ou altere as configurações do antivírus e demais ferramentas, a fim de não comprometer a segurança;

4.4. O sistema de proteção contra softwares maliciosos (antivírus, firewall, antispyware etc) será atualizado automaticamente no servidor e a atualização será replicada às estações de trabalho sempre que uma nova versão for disponibilizada pelo fabricante e homologada pelo setor responsável na TI;

4.5. A verificação periódica do disco rígido das estações de trabalho

software de antivírus será executada conforme agendamento definido pelo setor responsável na TI e será gerenciada automaticamente pelo servidor;

seja identificado impacto na estação/servidor decorrente execução da verificação do antivírus, o mesmo deve ser relatado Coordenação de TI para que o processo seja avaliado e alterado, se necessário;

odos os arquivos recebidos através da rede, mídia armazenamento, correio eletrônico, download ou páginas web deverão ser verificados automaticamente pelo antivírus antes serem utilizados;

ferramenta de antivírus deve ser configurada para que não seja possível a remoção ou alteração das configurações pelos usuários;

firewall pessoal das estações de trabalho deverá ser gerenciável bloquear o tráfego de entrada, com exceção das redes específicas dos colaboradores da TI que fazem a gestão segurança da informação, e em casos específicos onde seja justificada a necessidade (ex.: estações do suporte acessando porta de serviço de acesso remoto);

ambiente de tecnologia da informação da PGE-CE deverá instalado uma ferramenta de análise e correlação de eventos (SIEM);

estações de trabalho e servidores de rede deverão possuir agente configurado para o fornecimento de registros de log ferramenta de SIEM disponível no ambiente da PGE-CE;

o usuário perceba algum problema com os sistemas proteção (antivírus, firewall, SIEM, etc) em seu equipamento, este deverá entrar em contato com a Central de Serviços para sejam tomadas as devidas providências para a correção problema;

instalação de softwares ou aplicativos no ambiente da PGE-CE deverá ser realizada pela área técnica de TI, de forma a manter controle e evitar a introdução de vulnerabilidades ou outros incidentes relacionados a segurança da informação;

se tratarde um elemento de alto risco como ponto de entrada vulnerabilidades externas e para a fuga de informações corporativas, as portas USB dos notebooks e desktops deverão tratadas da seguinte maneira:

i. Como premissa básica, as portas USB não deverão ser utilizadas como dispositivos de dados (pen drives, HDs externos, drives de CD/DVD, outros) ou dispositivos portáteis (MTP), devendo estar, preferencialmente, desabilitadas nas estações de trabalho;
ii. Para liberação das portas USB, será necessário justificar o uso através de solicitação à Central de Serviços e ter aprovação do gestor imediato ou superior;
iii. Quando liberada a utilização da porta USB para uso de dispositivos de dados (pendrives, HDs externos, drives de CD/DVD, outros), os mesmos deverão ser automaticamente escaneados pela ferramenta de antivírus/antimalware antes de serem liberados para uso;
iv. Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que possa vir a causar nos ativos de informação;
v. Não será permitida a utilização da porta USB para conectar os seguintes dispositivos: modems, placas de rede externas (lan e/ou wifi), bluetooth, leitores de cartão.

4.15. A intenção de introduzir ou espalhar software malicioso no ambiente tecnológico da PGE-CE acarretará em sanções administrativas disciplinares e/ou contratuais aos seus respectivos usuários.