ANTIVÍRUS - INSTALAÇÃO, CONFIGURAÇÃO, UTILIZAÇÃO E ATUALIZAÇÃO

Sumário

ANTIVÍRUS - INSTALAÇÃO, CONFIGURAÇÃO, UTILIZAÇÃO E ATUALIZAÇÃO

1. ASSUNTO/OBJETIVO

Orientar a instalação, a configuração a utilização e a atualização dos antivírus deste Tribunal de Justiça.

2. FINALIDADE E ÂMBITO DA APLICAÇÃO

Garantir segurança aos sistemas e informações do TJPA, contra a execução de código hostil. Todas as Estações e Servidores ligados à rede do TJPA.

3. UNIDADE GESTORA

Serviço de Segurança e Sistemas Básicos (SSSB)

4. PÚBLICO ALVO

Magistrados, servidores, estagiários e os colaboradores em todas as unidades do TJPA.

5. RELAÇÃO COM OUTROS NORMATIVOS

SI-02.01- Política de Segurança da Informação

6. REGULAMENTAÇÃO UTILIZADA

NBR ISO 27002/2006.

7. DEFINIÇÕES E CONCEITOS BÁSICOS

Agente – é o módulo cliente instalado em todas as estações/servidores em uma organização e tem a função de prover uma comunicação segura entre o servidor de gerência e os softwares do servidor institucional de antivírus (atualmente Kaspersky) instalados em cada máquina;

Antivírus – programa cuja finalidade é detectar, isolar e, quando possível, remover códigos hostis em computador ou meio de armazenamento;

Arquivos de Atualização – arquivos utilizados pelo antivírus para atualização das definições de códigos hostis e do *engine*;

Central de Serviços – Central de Serviços de Tecnologia da Informação e Comunicação;

Chefia da Unidade – Servidor público que responde a função gratificada ou a cargo de confiança, responsável por coordenar as atividades de determinada unidade do TJPA;

Código Hostil – conjunto de instruções que tem como objetivo destruir, alterar, danificar ou se apropriar de informações não autorizadas. A ação do sistema de proteção objetiva que nenhum código hostil seja capaz de se auto-executar, sendo sempre necessário para tal a intervenção, intencional ou não, do usuário;

Download – processo de transferência de dados de um servidor para uma estação cliente;

Engine – nome dado pelos fabricantes de software antivírus para o conjunto de bibliotecas (.DLL) que contem os mecanismos de varredura e recuperação de arquivos infectados por vírus;

SSSB – Serviço de Segurança e Sistemas Básicos;

Software – Conjunto de instruções, logicamente organizadas em linguagem natural ou codificada, que capacitam máquinas na automatização e tratamento da informação para a execução de uma determinada tarefa;

Usuário – Magistrado, servidor, estagiário ou prestador de serviços autorizado a ter acesso aos recursos computacionais do TJPA para desempenho de suas atribuições;

Vírus – são pequenos programas, feitos geralmente em linguagem de máquina, que possuem a característica de se inserirem em outros programas passando a fazer parte deles, e de se replicarem automaticamente, contaminando (através de uma cópia de si mesmo) outros arquivos.

8. FLUXOS, FORMULÁRIOS E ORIENTAÇÕES TÉCNICAS

Não se aplica.

9. COMPETÊNCIAS E RESPONSABILIDADES

9.1 SSSB

9.1.1 Homologar padrões e procedimentos para instalação, configuração, utilização e atualização de antivírus.

9.1.2 Divulgar informações institucionais relacionadas à incidência de códigos hostis.

9.1.3 Prestar suporte e orientar Central de Serviços, sempre que necessário

9.1.4 Elaborar manuais técnicos com padrões e procedimentos para instalação, configuração, utilização e instalação de antivírus.

9.1.5 Definir a forma de distribuição dos arquivos de atualização do antivírus através da rede.

9.1.6 Efetuar captura, testes e disponibilização dos arquivos de atualização da plataforma antivírus para novos códigos hostis, sempre que houver liberação de novas versões pelo fabricante.

9.1.7 Comunicar a Central de Serviços, via correio eletrônico, quando da liberação de novas versões do antivírus.

9.1.8 Estabelecer e manter contato com o fabricante do antivírus para fins de suporte.

9.2 Central de Serviços

9.2.1 Instalar a versão mais atual do antivírus e dos arquivos de atualização conforme padrão definido nos manuais elaborados pelo SSSB.

9.2.2 Configurar os servidores e estações das redes locais para que seja efetuada atualização automática a partir da estação/servidor de atualização designado para a localidade.

9.2.3 Manter atualizados o antivírus e os arquivos de atualização nos servidores e estações de trabalho, utilizando para isso, somente os arquivos distribuídos pelo SSSB.

9.2.4 Instalar e manter atualizados o antivírus nos microcomputadores que não estejam conectados à rede.

9.2.5 Repassar e notificar o SSSB, sobre as ocorrências não solucionadas localmente.

9.2.6 Prestar atendimento ao usuário quanto a problemas relacionados à configuração, utilização e atualização de antivírus.

9.3 Usuário

9.3.1 Manter o antivírus instalado e ativo, nos equipamentos utilizados para desempenho de suas atribuições.

9.3.2 Acionar a Central de Serviços em caso de detecção de códigos hostis que não tenham sido removidos pelo antivírus.

9.3.3 Acionar a Central de Serviços em caso de problemas com a instalação e atualização do antivírus na estação.

9.4 Chefia da Unidade

9.4.1 Assegurar-se da existência de antivírus instalado atualizado e ativo, em todos os equipamentos da unidade sob sua responsabilidade.

10. PROCEDIMENTOS

10.1 PROCEDIMENTOS ASSOCIADOS AO ANTIVIRUS INSTITUCIONAL

10.1.1 A instalação inicial do antivírus e do agente Kaspersky Network nas estações está inclusa na imagem das máquinas

10.1.2 A atualização para novas versões do antivírus nas Estações de Trabalho e servidores será feita de forma automática e centralizada pelo SSSB.

10.1.3 Caso a instalação centralizada da nova versão apresente problemas a atualização do antivírus nas Estações de Trabalho e Servidores deve ser feita manualmente pela Central de Serviços de acordo com manual elaborado para esta finalidade.

10.1.4 Aplicativos de uso institucional que forem afetados (funcionamento inadequado/não funcionamento) após a instalação do antivírus, devem ser levados ao conhecimento da SSSB para sua análise, tratamento e liberação de suas funções em conjunto com a referida ferramenta.

11. RELATÓRIOS GERENCIAIS E INDICADORES

Relatórios de Infecção por Vírus

Relatório de Atualização de Base de Dados

Relatório de Versão do Kaspersky

12. CONSIDERAÇÕES FINAIS

Este normativo deve ser atualizado sempre que houver alteração nos procedimentos ou na ferramenta a ser utilizada. Demais esclarecimentos devem ser dirigidos ao Serviço de Segurança e Sistemas Básicos.

ANEXO I - PROCEDIMENTO OPERACIONAL PADRÃO PARA INSTALAÇÃO DO KASPERSKY ENDPOINT SECURITY 10 EM ESTAÇÕES DE TRABALHO.