

1. IDENTIFICAÇÃO

Padrão	Proteção de Estação de Trabalho e Servidores
Segmento	Segurança de TIC
Código	P02.001
Revisão	v. 2014

2. PUBLICAÇÃO

Versão	Data para adoção	Publicação
v. 2014	29 de dezembro de 2014	PORTARIA “N” Nº 232 de 23 de dezembro de 2014.
v. 2013	28 de dezembro de 2012	PORTARIA “N” Nº 182 de 27 de dezembro de 2012.

3. PROPÓSITO DO PADRÃO

A proteção de estação de trabalho e servidores visa mitigar os riscos em segurança da informação no ambiente computacional da Prefeitura da Cidade do Rio de Janeiro, no que se refere ao bloqueio de códigos maliciosos (*malware*), assegurando a disponibilidade, integridade, confiabilidade e autenticidade das informações que nele circulem. Sendo esta proteção realizada de forma corporativa, a fim de otimizar sua gestão e conformidade com a evolução tecnológica, garantindo a continuidade das atividades de negócio, assistência técnica e suporte.

4. RESPONSÁVEL PELO PADRÃO

Órgão	IplanRio
Diretoria	DOP - Diretoria de Operações
Setor	GIT - Gerência de Infraestrutura Tecnológica
Responsável	Gerente da GIT

5. DESCRIÇÃO DO PADRÃO

O padrão de proteção de estação de trabalho e servidores estabelece as aplicações que possuem funcionalidades que atendem a diferentes aspectos de segurança da informação, de modo a manter um ambiente computacional seguro. As aplicações componentes monitoram o fluxo de dados e bloqueiam ameaças digitais ao sistema da estação ou servidor, impedindo ação de códigos maliciosos, como, por exemplo, sites infectados, anexos de e-mails indesejáveis, arquivos corrompidos e dispositivos de acesso externos infectados. Sendo que para isso é fundamental que a base de dados utilizada por essas aplicações mantenha-se atualizada. As aplicações atuam como antivírus, *antispyware* e *antimalware*.

6. POLÍTICA E NORMATIZAÇÃO DE USO

- 6.1. Fica estabelecido como padrão tecnológico de Proteção de **Sistemas de Estações de Trabalho e Servidores** os itens listados na especificação técnica, para a promoção de um ambiente computacional seguro da Prefeitura da Cidade do Rio de Janeiro, no que se refere ao bloqueio de códigos maliciosos (*malware*);
- 6.2. Os componentes diferentes dos listados na especificação técnica e que estejam em execução no DataCenter ou nas estações de trabalho devem ser migradas para os componentes especificados como “Adotado”;
- 6.3. Cabe ao **responsável pelo padrão** monitorar a adoção deste padrão ou inconformidades no parque tecnológico da Prefeitura da Cidade do Rio de Janeiro, por meio de ferramenta específica para este fim;
- 6.4. Caso ocorram inconformidades, como não instalação das aplicações especificadas ou instalação de outros componentes que os listados na especificação técnica, a estação de trabalho ou servidor, deverá ser colocado em estado de quarentena até que se elimine a inconformidade, ou caso não seja cumprida a exigências, o equipamento em questão não poderá ser conectado à rede de dados da Prefeitura da Cidade do Rio de Janeiro;
- 6.5. Todas as exceções e dúvidas relacionadas a este documento devem ser tratadas com o **responsável pelo padrão**;
- 6.6. Com o objetivo de atualização, modernização e aumento da capacidade de atendimento as demandas, os componentes do padrão tecnológico **Proteção de Estações de Trabalho e Servidores** será revisto pela **Diretoria de Tecnologia da IplanRio** e pelo **responsável pelo padrão** com periodicidade de, no máximo, 365 dias a contar da data de publicação da portaria que o regulamenta.

7. ESPECIFICAÇÃO TÉCNICA

7.1. Especificação dos componentes:

Componente	Especificação	Situação
Ambiente Windows Servidor	SEP 12.x	Adotado
	SEP 11.x	Transição
Ambiente Windows estação de trabalho	SEP 12.x	Adotado
	SEP 11.x	Transição
Ambiente Linux Red Hat Servidor	SAVFL – Symantec Antivírus para Linux	Adotado
Ambiente Mac OS	SEP 12.x	Adotado
	SEP 11.x	Transição

7.2. Informações sobre os componentes adotados e recomendados

7.2.1.SEP – Symantec Endpoint Protection;

7.2.2.SAV para Linux – Symantec Antivírus para Linux: módulo antivírus do SEP, para sistemas operacionais baseados em Linux homologados pela Symantec para executar este cliente.

7.2.3.Fabricante dos componentes SEP e SAV: Symantec Corporate.

8. DEFINIÇÕES E ABREVIATÓES

Termo	Definição
SEP	Symantec Endpoint Protection – Proteção de ponto final Symantec
SAV	Symantec Anti-Virus – Symantec Antivírus
Vírus de computador	É um programa malicioso que infecta o sistemas computacionais, faz cópias de si mesmo e tenta se espalhar para outros computadores, utilizando-se de diversos meios.
Malware	É um software destinado a infiltrar-se em um sistema de computador de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não). Ele pode aparecer na forma de código executável, scripts de conteúdo ativo, ou em outros softwares.
Spyware	Consiste em um programa automático de computador, que recolhe informações sobre o usuário, sobre os seus costumes na Internet e transmite essa informação a uma entidade externa na Internet, sem o conhecimento e consentimento do usuário.
Adware	É qualquer programa que executa automaticamente e exibe uma grande quantidade de anúncios (ad= anúncio, software = programa) sem a permissão do usuário. As funções do Adware servem para analisar os locais de Internet que o usuário visita e lhe apresentar publicidade pertinente aos tipos de bens ou serviços apresentados lá.
Antivírus	Antivírus é um software responsável pela detecção, desinfecção e remoção de pragas digitais como vírus, trojans (cavalos de tróia), worms e qualquer outro tipo de código malicioso, não se limitando somente aos vírus. Atualmente alguns antivírus removem também adwares e spywares.
Anti-Spyware	Um anti-spyware é um software de segurança que tem o objetivo de detectar e remover adwares e spywares.
Anti-Malware	Um anti-malware é um software de segurança que tem o objetivo de detectar e remover malware.

9. REFERÊNCIAS

Symantec Endpoint Protection. Disponível em: http://en.wikipedia.org/wiki/Symantec_Endpoint_Protection. Acessado em: 17 de dezembro 2014.

Antivirus Software. Disponível em: http://en.wikipedia.org/wiki/Antivirus_software. Acessado em: 28 de dezembro 2014.

Spyware. Disponível em: http://en.wikipedia.org/wiki/Anti-spyware#Remedies_and_prevention. Acessado em: 17 de dezembro 2014.

Malware. Disponível em: <http://en.wikipedia.org/wiki/Malware>. Acessado em: 17 de dezembro 2014.

Personal firewall. Disponível em: http://en.wikipedia.org/wiki/Personal_firewall. Acessado em: 17 de dezembro 2014.

10 Motivos Para Escolher Antivirus Corporativo. Disponível em: <http://mundialshop.com.br/site/artigos-por-categoria/83-informatica-seguranca/129-10-motivos-para-escolher-antivirus-corporativo-em-vez-de-domestico-para-sua-empresa>. Acessado em: 17 de dezembro 2014.

Upgrading Symantec Endpoint Protection 11.x to version 12.1.x. Disponível em: <http://www.symantec.com/business/support/index?page=content&id=TECH207274>. Acesso em: 17 de dezembro 2014.

10. GRUPO TÉCNICO RESPONSÁVEL PELA ELABORAÇÃO DO PADRÃO

Diretoria de Tecnologia da IplanRio
Fernando Fernandes da Silva Caldeira

Diretoria de Operações da IplanRio
Jorge Francisco Antunes