

	Título	Código
	<b>POLÍTICA TÉCNICA DE AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO SEGURA DE SISTEMAS DE INFORMAÇÃO</b>	<b>EMAP-DCSGSI-13</b>
		Versão
		<b>0</b>
		Data
		<b>21/11/2019</b>
Elaborado por		Aprovado por
Ruan Louzeiro Santos		Thiago Drummond

## ÍNDICE

1. CONCEITOS E DEFINIÇÕES .....	1
2. REFERÊNCIAS LEGAIS E NORMATIVAS .....	1
3. OBJETIVO .....	1
4. DIRETRIZES GERAIS .....	2
5. REVISÕES .....	5

### 1. CONCEITOS E DEFINIÇÕES

- **Sistema de informação:** Programa de computador composto por uma sequência de instruções, que é interpretada e executada por um processador ou por uma máquina virtual.

Observar demais definições na Política de Segurança da Informação da EMAP.

### 2. REFERÊNCIAS LEGAIS E NORMATIVAS

Observar referências legais e normativas na Política de Segurança da Informação da EMAP.

### 3. OBJETIVO

A política técnica de aquisição, desenvolvimento e manutenção segura de sistemas de informação faz parte de um conjunto de documentos que compõem a Política de Segurança da Informação da EMAP. Os detalhes de determinados assuntos contidos nessa política técnica estão regulados em outras políticas técnicas.

- Esta política deve ser lida por todos empregados e prestadores de serviços que atuem com as atividades descritas nela.

A política técnica de aquisição, desenvolvimento e manutenção segura de sistemas de informação institui regras de segurança para processo seguro do ciclo de vida dos sistemas de informação da EMAP.

- Instituir orientações ao setor de TI no estabelecimento de medidas de segurança da informação que devem ser incorporadas ao processo de desenvolvimento e/ou implementação de sistemas de informação.
- Esta política técnica considera que os requisitos de segurança devem ser identificados e acordados antes do início de desenvolvimento e/ou implementação de sistemas de informação.
- Todos os requisitos de segurança devem ser identificados na fase de levantamento de requisitos dos projetos, sendo justificados, acordados e documentados como parte dos artefatos de negócio dos sistemas de informação.

## **4. DIRETRIZES GERAIS**

### **4.1. Requisitos de segurança de sistemas de informação**

A EMAP deve instituir definições de segurança da informação no desenvolvimento de novos sistemas de informação.

- Todo o ciclo de desenvolvimento de sistemas deve ter requisitos de segurança da informação definidos desde a definição, projeto, desenvolvimento, implantação e manutenção.
- Os sistemas de informação existentes na empresa devem passar por revisão para se adequar aos requisitos de segurança definidos pela empresa, quando possível.
- Os contratos de customizações de sistemas de informações desenvolvidas para uso exclusivo da EMAP devem possuir uma cláusula instituindo propriedade da empresa.
- A EMAP deve instituir um acordo de confidencialidade com empresas prestadoras de serviço e com empregados e prestadores de serviços que manuseiam códigos-fonte e base de dados dos sistemas desenvolvidos na empresa.

A EMAP deve instituir definições de segurança da informação no processo de aquisição sistemas de informação.

- A EMAP deve instituir em seus contratos que todas as customizações de sistemas de informações desenvolvidas para uso exclusivo da empresa, é de propriedade da EMAP.
- Um processo de verificação de segurança dos sistemas de informação após a

aquisição pela EMAP deve ser definido e automatizado.

- A EMAP deve instituir um acordo de confidencialidade com todas empresas fornecedoras de sistemas de informação.

#### **4.2. Segurança no processo de desenvolvimento**

A EMAP deve instituir procedimentos de verificação do funcionamento da infraestrutura de desenvolvimento após as atualizações ou substituições de sistemas de informações.

- Procedimentos de verificações do funcionamento dos sistemas de informações instalados na infraestrutura devem ser definidos.

O desenvolvimento de sistemas de informações realizados por prestadores de serviço deve ser supervisionado integralmente pelos empregados da EMAP.

- Cada sistema de informação desenvolvido para EMAP deve ter um empregado responsável designado.

A EMAP deve instituir um processo de identificação e versionamento de todos os sistemas de informação desenvolvidos.

- A identificação e o versionamento devem ser únicos.
- As ferramentas de desenvolvimento utilizadas na EMAP para a geração de sistemas de informação devem ser especificadas e identificadas claramente, desde a análise de requisitos e modelagem até a programação e testes.

Todos os sistemas de informações desenvolvidos pela/para EMAP devem ter um plano de documentação bem definidos.

- As documentações devem fornecer evidências de quais medidas de segurança foram adotadas durante o processo de desenvolvimento.
- As evidências devem garantir que as medidas são suficientes para manter a integridade e confidencialidade dos sistemas de informação.

#### **4.3. Segurança dos arquivos de sistemas**

A massa de dados utilizadas nos testes de desenvolvimento e homologação devem ser diferentes da utilizada no ambiente de produção.

- O processo de geração de massa de dados, preferencialmente, deve ser automatizado para criar informações aleatórias e que não reflitam dados de produção.

O acesso aos códigos fontes dos sistemas de informações da EMAP deve ser

controlado e autorizado.

- Os acessos aos códigos fontes devem ser concedidos considerando o princípio de privilégio mínimo.

A EMAP deve instituir procedimentos de instalação dos sistemas de informações.

#### **4.4. Gestão de vulnerabilidades técnicas**

A EMAP deve instituir um processo de gestão de vulnerabilidade técnica dos sistemas de informação adquiridos e/ou desenvolvidos pela/para a empresa.

- O processo de gestão de vulnerabilidade técnica deve ser automatizado para garantir maior efetividade da gestão.
- As informações sobre vulnerabilidades técnicas dos sistemas de informação devem ser adquiridas em tempo hábil a exposição da EMAP a estas vulnerabilidades.
- As vulnerabilidades técnicas identificadas devem ser avaliadas e medidas apropriadas devem ser tomadas para reduzir os riscos associados.

#### **4.5. Processamento correto de aplicações**

Os sistemas de informações devem ter seus dados de entrada validados para garantir que são corretos e apropriados.

- A validação deve ser realizada com vistas a detectar falta de integridade das informações, por erros ou ações intencionais.

A EMAP deve instituir controles para garantir a autenticidade e proteger a integridade das informações que trafegam nos sistemas de informações adquiridos e/ou desenvolvidos para/pela empresa.

Os sistemas de informações devem ter seus dados de saída validados para garantir que o processamento das informações estão corretos e são apropriados.

#### **4.6. Gestão de capacidade**

A EMAP deve instituir um processo de gestão de capacidade de sistemas de informações para reduzir riscos de sobrecarga de sistemas.

- Todos os sistemas de informações da EMAP devem ter estudos de viabilidade técnica e levantamento de requisitos definidos.

- Procedimentos de verificação de capacidade da infraestrutura de TI, utilizados na instalação dos sistemas de informação devem ser instituídos para reduzir os riscos de falhas de desempenho.

O processo de gestão de capacidade deve ser revisado em intervalos planejados, de acordo com a política definida pelo setor de TI.

#### **4.7. Disposições Finais**

- Os casos não previstos nesta política técnica deverão ser encaminhados para o setor de TI.
- Os casos omissos serão resolvidos pelo setor de TI.

### **5. REVISÕES**

Não se aplica.