POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE EDUCAÇÃO DE PERNAMBUCO

PC05 – POLÍTICA DE AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÕES

Faça disso um hábito!

HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
15/02/17	1.0	Versão elaborada e publicada	Equipe de Elaboração
31/07/18	2.0	Versão revisada	Equipe de Elaboração

SUMÁRIO

INTRODUÇÃO

A informação é o elemento básico, considerado dentro da SEE-PE como algo valioso, de maneira que os sistemas de informação e aplicações que a manipulam precisam evoluir para manter suas características iniciais disponíveis e confiáveis.

Os usuários interagem entre si e com a informação, modificando-a, de forma que deve haver uma cobertura clara sobre ações que podem ou não ser realizadas, agregando segurança a esse procedimento. Isto porque os dados podem ser alvo de uma série de ameaças com a finalidade de explorar as vulnerabilidades e causar prejuízos consideráveis à SEE-PE.

Assim, a presente Política de Segurança da Informação visa trazer orientações quanto à aquisição, ao desenvolvimento e à manutenção de Sistemas de Informações, de forma que haja um alinhamento técnico de acordo com uma metodologia de conhecimento da SEE-PE, estabelecendo as exigências mínimas a serem atendidas. Para tanto, serão abordados requisitos gerais, direcionadores e documentos de referência.

OBJETIVO

Definir a política de segurança que deve ser norteadora na aquisição, desenvolvimento e manutenção de sistemas de informação, visando assegurar a disponibilidade e continuidade dos serviços prestados por estes sistemas, minimizando os riscos do negócio e garantindo a confidencialidade, integridade e disponibilidade dos dados.

ABRANGÊNCIA

Esta política se aplica a todos os colaboradores da SEE-PE, quais sejam: funcionários servidores ou comissionados, estagiários, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, a infraestrutura ou as informações da SEE-PE. Todos os esses colaboradores serão tratados nesta política como usuários.

DIRETRIZES DE AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

1. Diretrizes Gerais

a. Os processos de aquisição, desenvolvimento e manutenção dos sistemas de informação devem seguir metodologia formal, a partir de uma análise crítica, que contemple aspectos relacionados às exigências legais vigentes e de segurança da informação;

b. Toda aquisição, desenvolvimento e manutenção de sistemas de informação deve ser submetido a um processo de gestão de mudança de forma a garantir o controle efetivo das modificações realizadas nos diversos ambientes, com o objetivo de registrar, avaliar e autorizar qualquer modificação nos sistemas de informação;

2. Diretrizes de Aquisição

a. A área de tecnologia da informação da SEE-PE será responsável por liderar as práticas para descrição técnica detalhada do produto ou serviço a ser adquirido;

b. A SEE-PE deve sempre elaborar um estudo de viabilidade, contendo um detalhamento das soluções analisadas para justificar a escolha da contratação de sistemas;

c. O estudo de viabilidade deve prever que qualquer modificação realizada por usuário externo à SEE-PE, com o escopo de gerar uma nova versão do sistema de informação, deve ser homologada e implantada, conforme o processo de gestão de mudança, mesmo visando correções de falhas neste produto;

d. As atividades de transição contratual, quando aplicáveis, e de encerramento do contrato devem estabelecer em suas cláusulas, no mínimo:

   I. A entrega de versões finais dos produtos e da documentação;
   II. A transferência final de conhecimentos sobre a execução e a manutenção da Solução de Tecnologia da Informação;
   III. A revogação de perfis de acesso;
   IV. A eliminação de caixas postais.

e. Em caso de encerramento não planejado do contrato pela empresa contratada (ex.: falência da contratada), esta deve fornecer os dados atualizados da SEE-PE na forma estabelecida contratualmente.

3. Diretrizes de Desenvolvimento e Manutenção de Sistemas de Informação

a. Todo sistema de informação deve passar por um processo de classificação, conforme Política de Classificação da Informação;

   I. A classificação da informação tratada pelos sistemas de informação definirá o local de hospedagem dos dados tratados;

   II. A classificação da informação deve definir qual acessibilidade ao dado em sua origem e formato;

   III. A depender da classificação obtida, o sistema de informação deve passar por uma validação de segurança, visando minimizar os riscos, encontrar possíveis vulnerabilidades e garantir a aderência dos sistemas de informação às normas de segurança de informações;

   IV. Será obrigatória a assinatura de Termo de Responsabilidade e/ou Acordo de Confidencialidade por parte dos prestadores de serviços, contendo declarações que permitam aferir que os mesmos tomaram ciência das normas de segurança vigentes da SEE-PE, garantindo que os dados disponíveis na aplicação só possam ser acessados pelos usuários autorizados.

b. O backup corporativo relacionado aos sistemas de informações, bem como sua frequência e retenção, deve ser definido, conforme o nível de confiabilidade em que foram classificados, conforme Política de Classificação da Informação;

c. O acesso aos ambientes de desenvolvimento, teste, homologação e produção será restrito apenas aos perfis definidos pela SEE-PE;

d. As bases de dados dos ambientes de produção, homologação, testes e desenvolvimento devem ser utilizadas especificamente para suas respectivas funcionalidades. Não sendo permitida a utilização de uma base de dados para funcionalidades diferentes da especificada;

e. Para que um sistema de informação seja utilizado no âmbito da SEE-PE, quando não produzido pela própria SEE-PE, os requisitos e contratos de licenciamento devem ser analisados, indicando o proprietário da aplicação e a forma adequada de uso, em concordância com a lei de direitos autorais, bem como o tempo de vigência do contrato;

f. Todo e qualquer evento de segurança detectado deve ser reportado para Central de Serviços, onde será categorizado, priorizado e tratado pela equipe de resposta a incidentes, conforme o Plano de Recuperação de Desastre e/ou Plano de Continuidade do Negócio.

g. A SEE-PE definirá uma metodologia de desenvolvimento e manutenção de sistemas de informação que deve ser seguida observando-se suas formalidades, necessidades de documentação e utilizações de ferramentas de gestão;

h. Deve ser adotado procedimento de mascaramento de dados dinâmicos para todo dado classificado como confidencial, de acordo com a Política de Classificação da Informação, limitando a exposição destes dados confidenciais para usuários sem privilégios;

i. Antes de disponibilizar nova versão de uma aplicação para o ambiente de produção, faz-se necessário que o usuário realize testes de validação e formalize a homologação para posterior liberação da sua entrada em produção;

j. Com o objetivo de minimizar os riscos e restringir acessos indevidos, o ambiente de produção será acessado apenas por usuários que têm autorização do gestor da área;

k. Uma equipe de gestão de mudança multidisciplinar deve ser estabelecida para garantir a efetividade do processo de gestão de mudança, analisar o impacto e minimizar os riscos de uma modificação em ambientes diversos;

l. A atualização dos códigos-fonte deve ser efetuada apenas após autorização formal, seguindo procedimentos de controle de mudança e versão;

m. Para garantir a continuidade, segurança e evitar mudanças não registradas e autorizadas em sistemas de informação, os acessos aos códigos-fonte devem ser restritos e controlados, inclusive para a área de infraestrutura;

n. Sempre que possível, o licenciamento utilizado para desenvolvimento e manutenção dos sistemas de informação não deve exigir o compartilhamento de código-fonte.

o. Deverão ser suprimidos os comentários com informações sensíveis que forem disponibilizados no código da linguagem de programação da internet (HTML) gerado.