POLÍTICA DE DESENVOLVIMENTO DE SOFTWARE

INTRODUÇÃO

A informação é o elemento básico considerado dentro da Câmara Municipal de Jundiaí como ativo 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 Câmara Municipal de Jundiaí.

Assim, a presente política visa trazer orientações quanto à aquisição, o desenvolvimento e a manutenção de Sistemas de Informações, de forma que haja um alinhamento técnico de acordo com uma metodologia de conhecimento da Câmara Municipal de Jundiaí que estabeleça as exigências mínimas a serem atendidas.

OBJETIVO

Definir a política 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 ao negócio e garantindo a confidencialidade, integridade e disponibilidade dos dados.

ABRANGÊNCIA

Esta política se aplica a todos os colaboradores da Câmara Municipal de

Jundiaí, quais sejam: servidores efetivos ou comissionados, estagiários, menores aprendizes, terceirizados, fornecedores de produtos e/ou serviços, ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações da Câmara Municipal de Jundiaí.

Todos os esses colaboradores serão tratados nesta política como usuários.

DIRETRIZES DA AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

Seguem abaixo as diretrizes gerais para nortear os processos de aquisição, desenvolvimento e manutenção de sistemas de informação.

GERAL

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.

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. Será obrigatória a assinatura de Termo de Compromisso 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 Câmara Municipal de Jundiaí, garantindo que os dados disponíveis na aplicação só possam ser acessados pelos usuários autorizados.

O backup corporativo relacionado aos sistemas de informações, bem como sua frequência e retenção, estão definidos na Política de Backup e restauração.

O acesso aos ambientes de desenvolvimento, teste, homologação e produção será restrito apenas aos perfis definidos pela Câmara Municipal de Jundiaí.

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

Para que um sistema de informação seja utilizado no âmbito da Câmara Municipal de Jundiaí, quando não produzido pela própria Câmara Municipal de Jundiaí, 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.

Todo e qualquer evento de segurança detectado deve ser reportado para área responsável onde será categorizado, priorizado e tratado por equipe designada pelo gestor da área, definindo-se um Procedimento para gerenciar violações.

ARMAZENAMENTO

Armazenar de forma segura os dados de usuários e os sistemas que utilizam cada senha fornecida, preferencialmente dados criptografados, utilizar meio que possua acesso por senha.

Não disponibilizar às aplicações acesso à algum banco de dados utilizando login de usuário com permissões além das estritamente necessárias ao seu funcionamento.

SENHAS

A elaboração de senhas deve seguir os padrões estabelecidos nas políticas internas, utilizando caracteres especiais, letras e números.

Não utilizar as mesmas senhas para ambientes de desenvolvimento, teste, homologação e produção.

Não se deve enviar a senha antiga para o usuário.

Periodicidade de troca: 6 meses.

ACESSO

Deve-se utilizar controle de usuário e senha nominais para determinar a identidade e autenticação via Active Directory sempre que possível para autenticar usuários internos.

Em caso de HTTP que utiliza cookies para manter sessões de usuário, faz-se necessário garantir tanto a segurança da troca de credenciais quanto a segurança das demais páginas acessadas pelos usuários dos sistemas web. O protocolo HTTPS visa contribuir para que essa segurança seja garantida, dessa forma deve-se utilizar HTTPS em todas as telas dos sistemas.

COMUNICAÇÃO

Utilizar canal de comunicação com controle de duplicação e perda de informações, com controle de autenticação (HTTPS, certificados digitais gerados por autoridades confiáveis, VPNs).

SEGURANÇA DA INFORMAÇÃO

Restringir permissões de acesso ao banco de dados para o usuário da aplicação.

Realizar testes de intrusão nas ferramentas.

BACKUPS

Definir um procedimento estruturado para a restauração de backups. Manter baselines das versões do sistema, facilitando a recuperação ágil para uma versão anterior.

AVALIAÇÃO

Realizar testes manuais de segurança antes de cada versão do software que modifique sua estrutura (telas de login, serviços não autenticados, novos formulários com interação com o usuário etc.).

DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

A Câmara Municipal de Jundiaí definirá uma metodologia de desenvolvimento e manutenção de sistemas de informação que deve ser seguida observando-se suas formalidades, necessidades de documentação de software e utilizações de ferramentas de gestão.

A base de dados do ambiente de homologação deve ser especificamente para testes.

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.

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.

O Setor de Informática deverá garantir a efetividade do processo de gestão de mudança, analisar o impacto e minimizar os riscos de uma modificação em ambientes diversos.

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

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.

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

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

AQUISIÇÃO

O Setor de Informática da Câmara Municipal de Jundiaí será responsável por liderar as práticas para descrição técnica detalhada do produto ou serviço a ser adquirido.

A Câmara Municipal de Jundiaí deve sempre elaborar um estudo de viabilidade contendo um detalhamento das soluções analisadas para justificar a escolha da contratação de sistemas.

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

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.

Em caso de encerramento não planejado do contrato (ex.: falência da contratada, aplicação de sanção administrativa, etc.), a empresa contratada será obrigada a fornecer os dados atualizados da Câmara Municipal de Jundiaí na forma estabelecida contratualmente.

ADEQUAÇÃO À POLÍTICA

Os novos projetos ou novas aquisições seguirão os padrões estabelecidos nesta política;

O ambiente tecnológico existente deverá ser adequado a esta política no prazo de 1 (um) ano, a partir de sua publicação;

Caso não seja possível a adequação do recurso técnico ou processo correspondente no prazo indicado, o Setor de Informática deve ser formalmente comunicado do fato e do motivo para fins de auditoria e outras medidas cabíveis em consonância com o interesse público.