POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação estabelece diretrizes que permitam à Câmara Municipal de Jundiaí salvaguardar seus ativos de informação, e implementação de controles e procedimentos para reduzir incidentes.

Todos os servidores devem definir seus direcionamentos a partir das orientações previstas na Política, considerando as necessidades específicas e os aspectos legais e regulamentares a que estão sujeitas.

O órgão, para manter a segurança da informação, exerce suas atividades baseadas nos seguintes pilares:

Confidencialidade: As informações só podem ser acessadas por pessoas autorizadas.

Integridade: As informações só podem ser alteradas por pessoas autorizadas.

Disponibilidade: As informações estarão disponíveis sempre que for necessário.

Autenticidade: As informações são verídicas, proveniente da fonte original e não foi alvo de alteração.

Conformidade: Os processos do órgão estão de acordo com os regulamentos, normativos e leis vigentes, de forma a seguir todos os protocolos exigidos na Câmara.

A Câmara considera ativos de informações todas as informações geradas ou desenvolvidas no órgão, tais como: arquivos digitais, consentimentos de munícipes e servidores, equipamentos, mídias externas, documentos impressos, documentos assinados digitalmente, sistemas, dispositivos móveis, banco de dados, conversas

e gravações. Os ativos devem ser utilizados apenas para a sua finalidade devidamente autorizada, sendo sujeito a monitoramento ou auditoria.

Sobre a segurança cibernética a Câmara resguarda a proteção dos dados contra acessos indevidos, bem como contra modificações, exclusões ou divulgações não autorizadas, realiza a adequada classificação das informações e mantem a continuidade do processamento das mesmas, conforme os critérios e princípios indicados nos procedimentos internos, mantem os sistemas e dados devidamente protegidos e utilizados apenas para o cumprimento de suas atribuições.

Com relação às medidas de segurança, adota procedimentos e controles para reduzir a vulnerabilidade do órgão a incidentes e atender aos objetivos de segurança, dentre eles: a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de varreduras para detecção de vulnerabilidades.

É necessário o cumprimento da Política, e responsabilidade de cada servidor compreender sobre a segurança da informação em suas atividades.