Governação das TIC na Administração Pública Local – Propostas para a Segurança da Informação

ICT Governance in Local Government – Proposals for Information Security

Pedro Santos, ESTIG/Instituto Politécnico de Beja, Portugal, santos.pmcm@gmail.com

Isabel Sofia Sousa Brito, ESTIG/Instituto Politécnico de Beja, Portugal, isabel.sofia@ipbeja.pt

Resumo

Em Portugal no ano de 2012 foi elaborado o PGERRTIC (Plano Global Estratégico de Racionalização e Redução de custos nas TIC, na Administração Pública) com o objetivo de melhorar o serviço público, com um menor custo. Este plano enumera cinco grupos de medidas importantes a aplicar aos recursos TIC na administração pública, sendo eles: i) melhoria dos mecanismos de governação; ii) redução de custos; iii) utilização das TIC para potenciar a mudança e a modernização administrativa; iv) implementação de soluções TIC comuns; v) estimulo ao crescimento económico. No âmbito da garantia da informação e subsequente necessidade de segurança da informação este plano indica: i) racionalização, organização e gestão do setor; ii) arquitetura, normas e *guidelines* de tecnologias e sistemas de informação; iii) definição e implementação de uma estratégia nacional de segurança da informação; e iv) definição e implementação de planos de ação setoriais de racionalização das TIC.

Este trabalho tem como objetivo endereçar algumas dessas medidas no âmbito da garantia e segurança da informação, associada especificamente à administração local. Para alcançar este objetivo propõe-se a criação de uma EGTIC (Estrutura de Governação para as Tecnologias de Informação e Comunicação). Esta proposta assenta nas boas práticas existentes a nível mundial no que diz respeito à governação e gestão das TIC e segurança nos sistemas de informação. A integração da governação das TIC na governação do município e reconhecer o papel de parceiro de negócio no desenvolvimento de soluções e novas áreas para gerar valor público, apoia a transparência fundamentada no uso de normas e frameworks reconhecidos internacionalmente. Assim pretende-se o reconhecimento das TIC como parceiros de negócio e fonte de criação de valor, ao invés de unicamente fonte de suporte ao mesmo negócio. Este reconhecimento terá como consequência a integração da governação das TIC na governação do município.

A proposta para a implementação da EGTIC no município é baseada no guia de implementação do CobiT 5. Este guia também orienta o programa de implementação e a forma de concretizar cada uma das fases do ciclo de melhoria contínuo, incluindo a forma de utilizar outras ferramentas tais como o ITIL ou a ISO/IEC 27000. Usando o "Appendix D. Example Business Case" do guia de implementação do CobiT 5, assim como as matrizes fornecidas pelo mesmo guia e pelo próprio *Framework* é realizada uma análise da capacidade e das necessidades do município antes de iniciar a implementação da EGTIC. Nesta análise é importante identificar os participantes que deverão estar envolvidos no programa, e que deverão ser partes interessadas chave no mesmo.

O referido programa de implementação de uma estrutura de governação é aplicado em simultâneo com a primeira iteração do ciclo de melhoria contínuo constituído por sete fases. Este ciclo irá dar início à capacitação dos processos do município, incluindo os processos relativos à segurança e garantia da informação.

A aplicação do programa de implementação permitiu chegar a algumas conclusões, tais como, i) a morosidade de cada interação do programa; ii) a necessidade da mitigação de alguns

ISSN 2183-489X
DOI http://dx.doi.org/10.18803/capsi.v17.00-00

riscos, como por exemplo, o necessário apoio do executivo; iii) a identificação de atividades relevantes na área da segurança e garantia da informação; iv) a segurança da informação é salvaguardada ao nível do risco assumido, garantindo-se a otimização dos recursos com a priorização (pela EGTIC) baseada em justificações estratégicas; v) a criação do desejo de agir perante os resultados da análise de capacidade do município/processos.

Na perspetiva da segurança e garantia da informação foram identificadas uma série de atividades relevantes e que remetem diretamente para a gestão de risco, segurança da informação e garantia dos dados, a saber:

- Classificação dos dados, porque é importante classificar todo o tipo de dados sensíveis e o fluxo que estes possuem dentro do sistema como um todo. Neste ponto também se julga importante que o município tenha forma de conhecer o ciclo de vida de todos os seus ativos de informação.

- Monitorizar e avaliar os fornecedores quanto à conformidade com políticas existentes assegurando as condições de segurança da informação e cumprimento dos contratos e *Service Level Agreement* (SLA), garantindo que os incidentes de segurança são geridos da forma correta.

- É considerado essencial que seja usado uma metodologia baseada na análise de risco para priorizar as respostas às falhas de segurança de uma forma rápida, reduzindo assim ao mínimo ou mesmo eliminar o impacto no município ou partes interessadas.

- A necessidade de um Sistema de Gestão da Segurança da Informação (SGSI) que forneça uma perspetiva coordenada de segurança da informação para o município, e permitir implementar controlos de uma forma coerente. A segurança da informação é obtida através da implementação de um conjunto adequado de controlos, incluindo políticas, processos, procedimentos e estruturas organizacionais. Estes controles precisam ser estabelecidos, implementados, monitorizados, revistos e melhorados, sempre que necessário, para garantir que os objetivos de segurança e de negócios específicas do município possam ser alcançados.

- Qualquer organização deve prevenir-se, de forma eficaz, contra a manipulação maliciosa de dados sensíveis, tanto do ponto de vista de rede informática como do utilizador.

- A monitorização de todo o processo ou controlos implementados permite garantir o cumprimento dos requisitos internos e externos estabelecidos.

Importa salientar a disseminação do conhecimento sobre o que é uma EGTIC e o seu contributo para uma governação pública melhor. Devemos destacar também a importância de nivelar as propostas de capacitação de soluções, sistemas ou processos através do uso de uma justificação estratégica com parâmetros comparáveis, permitindo assim a priorização do investimento.

Em outra vertente, e sendo conhecido que muitas vezes a aferição do estado dos serviços TIC e sistemas de informação existentes nos municípios é feito de forma ad hoc ou com recursos a auditores externos, mostrou-se que a utilização das ferramentas do CobiT 5 para efetuar essa análise de capacidade, é bastante reveladora e eficaz. Abre-se assim uma porta para a primeira fase de implementação da EGTIC, criar o desejo de agir.

Palavras-chave: (governação; CobiT 5; segurança da informação; administração pública)

Abstract

In 2012 the Portuguese government has proposed the "Plano global estratégico de racionalização e redução de custos nas TIC, na Administração Pública" with the objective of improving the public service, at a lower cost. This plan is composed of a set of five important actions to be applied to Information and Communications Technology (ICT) resources in public administration: i) improvement of government mechanisms; ii) cost reduction; iii) use of ICT to promote change and government modernization; iv) implementation of common ICT solutions; v) stimulating economic growth. In the scope of information security, this plan indicates: i) ICT rationalization, organization and management; ii) information systems and technologies architecture, standards and guidelines; iii) definition and implementation of a

national information security strategy and, iv) definition and implementation of sectorial action plans to rationalize ICT.

This paper aims to address some of these actions in context of information assurance and security specifically associated with local government. To achieve this goal, the creation of a "Governance Information Technologies Structure" (GEITS) is proposed. This proposal is based on existing good practices at a global level in the government and management of ICT, ICT (Information Technology) and security of information systems. Integrating ICT management in local governments as well as recognizing the role of the business partners in solutions achievement and new areas development to create public value stands for the supported transparency in the use of rules and frameworks internationally recognized. Thus, appreciating ICT as business partners and a source of value creation rather than purely as a source of support to the business itself is the intention. The effect of this appreciation will be the integration of ICT management into the local governance.

The proposal for implementing the GEITS in the municipality is based on the CobiT 5 implementation guide. This guide also directs the implementation program and the method for incorporating each phase of the continuous improvement process, including how to use other tools such as ITIL or ISO/IEC 27000. A case study of its use appears in Appendix D. Example Business Case of the CobiT 5 implementation guide as well as the blueprints provided by the guide and the framework itself has led to some conclusions, such as i) the slowness of each program interaction; ii) the need to mitigate some risks, for example, the need of executive support; iii) the identification of relevant activities in the field of information security and assurance; iv) the security of the information is guaranteed according to the risk assumed thereby ensuring optimized resources with prioritization (through the GEITS) based on business cases; v) promote the desire to act when facing the results of the local government/processes capacity analysis.

From an information security and assurance perspective, a series of relevant activities have been identified referring directly to risk management, information security and data security, namely:

- To ensure that security incidents are managed properly the local government needs to assess suppliers for compliance with existing policies guaranteeing information security conditions and compliance with contracts and Service Level Agreement (SLA).

- To minimize or even eliminate the impact for local government or stakeholders is essential the use of a methodology based on risk analysis to improve security incident.

- The need for an Information Security Management System (ISMS) to provide a coordinated information security perspective for the local government and to enable the implementation of controls in a coherent manner. Information security is achieved through the implementation of an adequate set of controls, including policies, processes, procedures and organizational structures.

- Any organization must effectively prevent malicious manipulation of sensitive data.

- Checking the process or the implemented controls ensures compliance with internal and external requirements.

It is important to explain what an EGTIC is and how it contributes to better public governance. It is also important leveling the training proposals of solutions, systems or processes through the use of a strategic justification with comparable parameters, allowing the prioritization of investment.

Frequently the assessment of the ICT services and information systems in the government is done ad hoc or uses external auditors, the work presented in this paper shows that the use of CobiT 5 tools to carry out this capacity analysis is quite effective. This opens a door to the first phase of implementation of EGTIC, creating the desire to act.

Keywords: *governance; CobiT5; information security; local government*