Instituto Português de Corporate Governance

Governo societário de Sistemas de Informação

Proposta de princípios e recomendações para o governo societário de Sistemas de Informação

«Governo do Sistema de Informação: O conjunto de práticas relativas à tomada de decisões políticas e estratégicas através das quais a direcção e controlo do Sistema de Informação de uma sociedade são assegurados. O governo do Sistema de Informação é parte integrante do governo da sociedade e envolve: i) Avaliar as necessidades das partes interessadas para definir os objectivos do Sistema de Informação; ii) Dirigir através da priorização e tomada de decisão; e iii) Controlar o desempenho e a conformidade com a direcção e os objectivos estabelecidos.»

Versão Draft Final • 2 de Junho de 2015

Governo societário de Sistemas de Informação

Proposta de princípios e recomendações para o governo societário de Sistemas de Informação

Enquadramento

A Informação é hoje um dos principais activos nas Organizações e a capacidade dos seus Sistemas de Informação constitui cada vez mais factores competitivos de diferenciação e de criação de valor. No entanto, a crescente complexidade dos Sistemas de Informação, nas suas dimensões de Organização, Pessoas, Processos e, sobretudo, Tecnologias, exige aos responsáveis pelo governo das Organizações novas competências e a adopção de boas práticas susceptíveis de potenciar o contributo dos Sistemas de Informação para a satisfação das necessidades das partes interessadas, internas ou externas, e para a optimização dos riscos e dos recursos disponíveis.

De entre os diversos desafios relacionados com os Sistemas de Informação das Organizações, destacam-se os seguintes:

- Necessidade de alinhamento e integração entre o governo das sociedades e o governo do Sistema de Informação;
- Necessidade de alinhamento e integração dos objectivos e estratégias do Sistema de Informação com os objectivos e estratégias de negócio;
- Necessidade de definição de responsabilidades transversais no contexto do Sistema de Informação, designadamente dos órgãos de Governo, Gestão e Operação da sociedade;
- Necessidade de promover a consciencialização para as novas ameaças e oportunidades relacionadas com o Sistema de Informação, em particular as relacionadas com as novas Tecnologias de Informação e Comunicação (ex. *Cloud*, *Big Data*, Mobilidade, Ciber-riscos, Redes Sociais);
- Necessidade de garantir a conformidade do Sistema de Informação com os requisitos legais, normativos e contractuais;
- Necessidade de adaptação das Organizações a novos modelos de exploração e crescente importância do governo e gestão de entidades externas (ex. *outsourcing*);

Governo do Sistema de Informação

«O conjunto de práticas relativas à tomada de decisões políticas e estratégicas através das quais a direcção e controlo do Sistema de Informação de uma sociedade são assegurados.

O governo do Sistema de Informação é parte integrante do governo da sociedade e envolve: i) Avaliar as necessidades das partes interessadas para definir os objectivos do Sistema de Informação; ii) Dirigir através da priorização e tomada de decisão; e iii) Controlar o desempenho e a conformidade com a direcção e os objectivos estabelecidos.»

- Necessidade de valorização do factor humano nos Sistemas de Informação, nomeadamente na qualificação, requalificação ou actualização de competências para alinhamento com as necessidades; e
- Crescente importância de promover uma cultura, conduta profissional e ética, também no contexto do Sistema de Informação.

Tendo este contexto como ponto de partida, e atendendo à missão do Instituto Português de Corporate Governance (IPCG) de endereçar os mais variados temas que, de forma directa ou indirecta, possam ter impacto na adopção de boas práticas de *Corporate Governance*; a Direcção do IPCG decidiu criar um grupo de trabalho para preparação e discussão de uma proposta de princípios e recomendações para o bom governo societário de Sistemas de Informação.

Destinatários

O documento tem como destinatários os titulares dos órgãos de governo das Organizações em Portugal, em particular os órgãos de Administração e Fiscalização, valorizando a sua função através da introdução de responsabilidades e competências relacionadas com o governo do Sistema de Informação.

No sentido de assegurar o correcto entendimento das responsabilidades, actividades e funções no contexto dos sistemas de governo das Organizações, o documento poderá ser igualmente útil para os titulares de cargos de gestão executiva ou outras partes interessadas com necessidades relacionadas com o Sistema de Informação.

Glossário

Para efeitos do presente documento, entende-se por:

Boa prática

Uma actividade ou processo utilizado por diversas Organizações e que tem demonstrado resultados confiáveis.

Criação de valor

O principal objectivo do governo de uma sociedade, atingido através do equilíbrio dos objectivos de i) satisfação de necessidades; ii) optimização dos riscos; e iii) optimização dos recursos.

Gestão do Sistema de Informação

O planeamento, organização, desenvolvimento, produção e controlo do Sistema de Informação em conformidade com a direcção definida pelo órgão de administração para cumprimento dos objectivos corporativos.

Gestor do Sistema de Informação

A função responsável pelo alinhamento e integração da estratégia do Sistema de Informação com a estratégia do negócio, bem como por planear, capacitar e gerir a entrega de serviços e soluções relacionadas com o Sistema de Informação para suportar os objectivos corporativos.

Governo da sociedade

O conjunto de responsabilidades e práticas exercidas pelo órgão de administração com o objectivo de dirigir a estratégica, garantir que os objectivos são alcançados, garantir que os riscos são geridos e controlar a utilização responsável dos recursos da sociedade.

Governo do Sistema de Informação

O conjunto de práticas relativas à tomada de decisões políticas e estratégicas através das quais a direcção e controlo do Sistema de Informação de uma sociedade são assegurados.

O governo do Sistema de Informação é parte integrante do governo das sociedades e envolve: i) Avaliar as necessidades das partes interessadas para definir os objectivos do Sistema de Informação; ii) Dirigir através da priorização e tomada de decisão; e iii) Controlar o desempenho e a conformidade com a direcção e os objectivos estabelecidos.

Informação

Dados com contexto que, como qualquer outro activo importante da sociedade, suporta as necessidades das actividades, da gestão e do negócio. A Informação pode existir em diversos formatos: impressa ou escrita em papel, armazenada fisicamente ou electronicamente, enviada por correio e por um meio electrónico ou ainda divulgada em conversas. A Informação pode ser estruturada ou desestruturada, formalizada ou não formalizada.

Entende-se por «Ciclo da Informação»: i) a produção de Dados pelos processos corporativos; ii) a transformação dos Dados em Informação através da sua contextualização; iii) a transformação de Informação em Conhecimento; e a utilização de Conhecimento para a criação de valor.

Objectivos corporativos

A tradução da missão da sociedade em objectivos e métricas de desempenho.

Objectivos do Sistema de Informação

A declaração que descreve o resultado esperado do Sistema de Informação no suporte aos objectivos corporativos.

Órgão de Administração

O conselho de administração, conselho de administração executivo ou outros casos previstos na lei e enquadrados no art.º 278º do Código das Sociedades Comerciais.

Órgão de Fiscalização

O conselho fiscal, nas sociedades que adoptem o modelo monista; a comissão de auditoria, nas sociedades que adoptem o modelo anglo-saxónico; o conselho geral e de supervisão, nas sociedades que adoptem o modelo dualista.

Qualidade da Informação

O conjunto de atributos do activo Informação que podem ser agrupados em:

- Qualidade intrínseca – Correcção; Objectividade; Credibilidade; e Reputação;
- Qualidade Contextual – Relevância; Totalidade; Actualização; Quantidade adequada; Representação concisa; Representação consistente; Interpretação; Compreensão; Facilidade de manipulação; Rendibilidade; e
- Segurança e Acessibilidade – Disponibilidade; Acesso restrito.

Tecnologia de Informação

O *hardware*, *software*, comunicações ou outras infra-estruturas utilizadas para registo, armazenamento, processamento e distribuição de dados em qualquer formato. Pode-se considerar o elemento tecnológico do Sistema de Informação.

Sistema de Informação

O conjunto de elementos (organizacionais, processuais, humanos e tecnológicos) que, mediante regras de relacionamento adequadas e fins previamente definidos, visam a produção, a armazenagem e o acesso à Informação.

Proposta de princípios e recomendações de boas práticas para o governo societário do Sistema de Informação

Princípios	Recomendações de boas práticas
Princípio 1 - O órgão de administração é responsável pelo governo do Sistema de Informação	a. O órgão de administração deve assumir a responsabilidade por i) avaliar; ii) dirigir; e iii) controlar o Sistema de Informação da sociedade. b. O órgão de administração deve garantir a valorização do factor humano através da promoção de uma cultura, ética e comportamentos desejáveis no contexto do Sistema de Informação, bem como da valorização de uma comunicação interna eficiente. c. O órgão de administração deve garantir a avaliação regular da eficácia e desempenho do Sistema de Informação e a articulação com o órgão de Fiscalização e demais funções fiscalizadoras (ex. auditor externo). d. O órgão de administração deve garantir que recebe toda a informação necessária para o cumprimento das suas responsabilidades relacionadas com o Sistema de Informação.
Princípio 2 - O órgão de administração é responsável pelo alinhamento e integração da estratégia do Sistema de Informação com a estratégia e objectivos do negócio	a. O órgão de administração deve garantir o alinhamento e integração das políticas, objectivos e estratégia do Sistema de Informação com as políticas, objectivos e estratégia da sociedade. b. O órgão de administração deve garantir que o Sistema de Informação contribui para a criação de valor na sociedade, nomeadamente na satisfação de necessidades das partes interessadas, optimização dos riscos e optimização dos recursos. c. O órgão de administração deve incentivar a apresentação de propostas de inovação relacionadas com o Sistema de Informação que permitam à sociedade responder a novas oportunidades ou desafios, desenvolvimento de novos negócios ou melhoraria dos processos. d. O órgão de administração deve garantir a afectação de recursos suficientes para que o Sistema de Informação suporte as necessidades e objectivos da sociedade, tendo em consideração as prioridades acordadas e os constrangimentos orçamentais.
Princípio 3 - O órgão de administração é responsável por delegar na gestão executiva a responsabilidade pela implementação de uma estrutura de suporte ao	a. O órgão de administração deve garantir a implementação dos princípios, políticas, estruturas organizacionais, processos e outros mecanismos necessários ao governo do Sistema de Informação. b. O órgão de administração deverá nomear um «Comité estratégico/arquitectura do Sistema de Informação» ou função semelhante de suporte ao governo e gestão do Sistema de Informação.

governo do Sistema de Informação	c. O órgão de administração deve nomear um «Gestor do Sistema de Informação» com a competência e experiência necessárias para o desempenho da função, devendo este comunicar regularmente em aspectos estratégicos do Sistema de Informação com o órgão de administração ou outros comités executivos.
Princípio 4. O órgão de administração é responsável por controlar e avaliar os investimentos e custos relevantes relacionados com o Sistema de Informação	a. O órgão de administração deve controlar o contributo do Sistema de Informação para a criação de valor da sociedade e controlar o retorno do investimento dos programas/projectos relevantes relacionados com o Sistema de Informação. b. O órgão de administração deve garantir a protecção da propriedade intelectual e a gestão do conhecimento relacionadas com o Sistema de Informação. c. O órgão de administração deve garantir a revisão periódica e independente do governo e gestão dos serviços externos relacionados com o Sistema de Informação.
Princípio 5. O órgão de administração é responsável por garantir que as oportunidades e ameaças relacionadas com o Sistema de Informação são parte integrante da gestão de risco da sociedade	a. O órgão de administração deve garantir que a gestão executiva demonstra periodicamente a existência de estratégias que assegurem a continuidade e resiliência operacional perante a ocorrência de eventos de ameaça relacionados com o Sistema de Informação. b. O órgão de administração deve garantir a conformidade do Sistema de Informação com requisitos legais, normativos, contratuais e boas práticas de referência. c. O órgão de administração deve garantir que as ameaças, oportunidades, preocupações, incidentes e problemas relacionados com o Sistema de Informação são identificados e reportados por qualquer pessoa e em qualquer momento. Estes riscos devem ser tratados em conformidade com as políticas e procedimentos aprovados e escalados para os decisores relevantes. d. O órgão de administração deve garantir a definição e implementação de uma estrutura de controlo interno do Sistema de Informação, bem como a verificação periódica independente da sua adequação e eficácia. e. Os comités de risco, auditoria ou funções similares deverão apoiar o órgão de administração nas suas responsabilidades pelo Sistema de Informação, em particular na avaliação e controlo dos riscos com impacto na operação do negócio, conformidade e reporte da informação financeira.
Princípio 6. O órgão de administração é responsável	a. O órgão de administração deve garantir a definição e implementação de práticas de gestão que garantam a qualidade da Informação ao

por garantir a gestão eficaz do activo Informação	longo do seu ciclo de vida, nomeadamente em áreas como a «privacidade e protecção dos dados», «segurança da informação» ou «gestão do conhecimento». b. O órgão de administração deve garantir que toda a Informação pessoal está identificada e é tratada como um activo importante da sociedade. c. O órgão de administração deve i) garantir a definição e implementação de um sistema de gestão da segurança da Informação adequado e eficaz; ii) aprovar os princípios, políticas e a estratégia de Segurança da Informação; e iii) atribuir as responsabilidades pela sua gestão.

Grupo de trabalho

Os elementos fundadores do grupo de trabalho «Governo societário de Sistemas de Informação»:

- Prof. Almiro de Oliveira, ISEG, UCP-Porto, Vice-Presidente e Fundador do ISGec/ceGSI, Presidente do ceGSI Portugal;
- Dr. Bruno Horta Soares, *Senior Advisor* em Governança e Gestão de Sistemas de Informação na GOVaaS e Presidente do ISACA Lisbon Chapter (Coordenador);
- Dr. Bruno Padinha (em representação da EY);
- Dr. João Carlos Frade (em representação da Deloitte);
- Dr. João Pedro Castro Mendes, Advogado;
- Dr. Luís Neto Galvão, Advogado, Sócio da SRS Advogados e membro do «Expert Group on Cloud Computing» da Comissão Europeia;
- Prof. Miguel Mira da Silva, Professor de Sistemas de Informação no Instituto Superior Técnico; e
- Dr. Rui Gomes (em representação da KPMG).

Referências

Na preparação do presente documento foram consideradas as seguintes boas práticas como referência:

- COBIT® 5, ISACA;
- Código de Governo das Sociedades do IPCG;
- ISO/IEC 38500;
- King Report on Corporate Governance (King III);
- Manifesto do Clube Europeu para a Governança dos Sistemas de Informação (ceGSI);
- OECD Principles of Corporate Governance , OECD, 1999 and 2004; e
- Report of the Committee on the Financial Aspects of Corporate Governance.