



Governo societário de Sistemas de Informação



Bruno Horta Soares, CISA®, CGEIT®, CRISC™, COBIT® 5 F, PMP®

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

16 de Junho de 2015 - IPCG



“É que só nos
faltava esta!”



6 Princípios e
22 recomendações



Próximos
passos

O seu mundo mudou?

É que só nos faltava esta!

"The reports of my death are greatly exaggerated"

Mark Twain

Organizações cada vez mais hiperconectadas e centradas em Informação



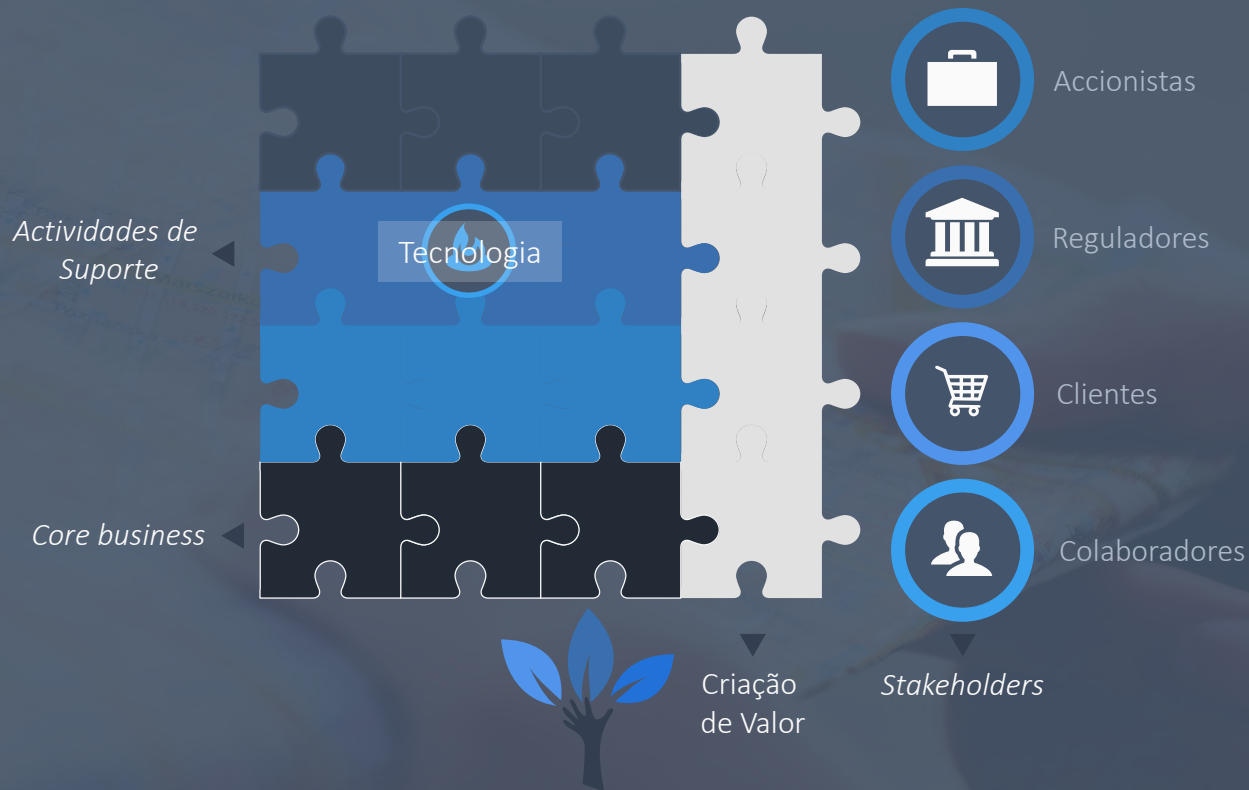
"Always-on"



Novas competências digitais... e escassez de competências!

No princípio era o negócio...

É que só nos faltava esta!





... depois veio a Informação

É que só nos faltava esta!



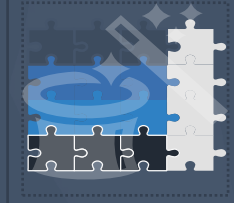
"Será que estamos em conformidade com todos os regulamentos aplicáveis?"

03

"Os Fornecedores TIC"

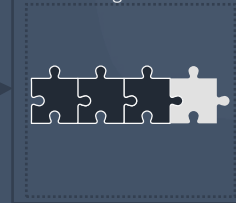
Organização

"Fornecedores"



Organização

"Negócio"



02

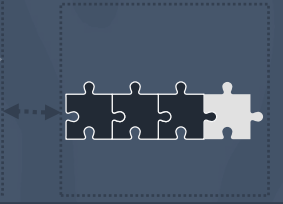
"Os Serviços de SI/TI"

Organização

"Serviços"



"Negócio"



"Clouds, Redes Sociais, Mobilidade, Big Data, Cyber Security... todas as semanas aparecem com uma diferente!"



"Ficámos um fim de semana sem sistema, de quem é a culpa?"



"A Informação que estou a receber é fidedigna? Podemos mesmo avançar?"

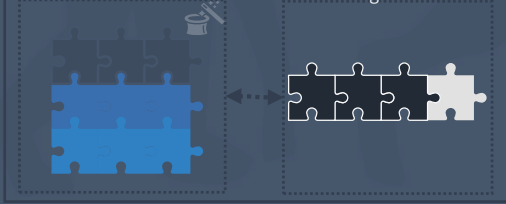


"A lista dos meus clientes VIP foi parar aos jornais, e agora?"

Organização

"Informática"

"Negócio"





Missão do grupo de trabalho

“Preparação de uma proposta de princípios e recomendações sobre o governo societário dos sistemas de informação alinhadas com as boas práticas de corporate governance e destinadas aos órgãos de administração e fiscalização das sociedades em Portugal.”

Tecnologias vs. “Sistemas de Informação” vs. Sistema de Informação

6 Princípios e 22 Recomendações

*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.”*



Visão geral da proposta

6 Princípios e 22 Recomendações

P#1

Responsabilidade

“O órgão de administração é responsável pelo governo do Sistema de Informação”

4

P#2

Estratégia

“O órgão de administração é responsável pelo alinhamento e integração da estratégia do Sistema de Informação com a estratégia e objectivos do negócio”

4

P#3

Organização

“O órgão de administração é responsável por delegar na gestão executiva a responsabilidade pela implementação de uma estrutura de suporte ao governo do Sistema de Informação”

3

P#4

Capacitação

“O órgão de administração é responsável por avaliar e controlar os investimentos e custos relevantes relacionados com o Sistema de Informação”

3

P#5

Risco e Conformidade

“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”

5

P#6

Informação

“O órgão de administração é responsável por garantir a gestão eficaz do activo Informação”

3

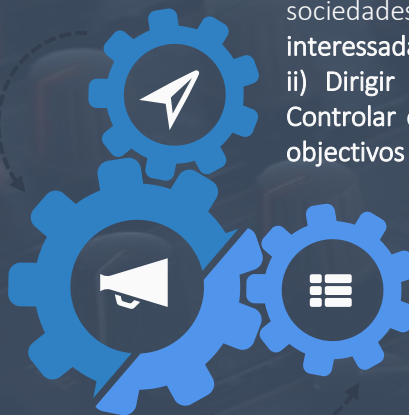
P#1 - Responsabilidade

6 Princípios e 22 Recomendações



Gestão do Sistema de Informação

“A responsabilidade pelo planeamento, organização, desenvolvimento, operação e controlo do Sistema de Informação em conformidade com a direcção definida pelo órgão de Administração para cumprimento dos objectivos corporativos.”



Governo Societário 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.**”

Operação do Sistema de Informação

“A **execução e reporte de actividades** de planeamento, organização, desenvolvimento, operação e controlo em alinhamento com as instruções da Gestão.”

Recomendações

1.1 O órgão de administração deve assumir a responsabilidade por i) avaliar; ii) dirigir; e iii) controlar o Sistema de Informação da sociedade.

1.2 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.

1.3 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).

1.4 O órgão de administração deve garantir que recebe toda a informação necessária para o cumprimento das suas responsabilidades relacionadas com o Sistema de Informação.

P#1

Responsabilidade



P#2 - Estratégia

6 Princípios e 22 Recomendações



Recomendações

2.1 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.

2.2 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.

2.3 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.

2.4 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.

P#2

Estratégia



P#3 - Organização

6 Princípios e 22 Recomendações



Drs. | ~~Negócio~~ | Funções de Governança e Gestão do SI



Engs. | ~~"Informática"~~ | Funções de Operação do SI

Recomendações

3.1 O órgão de administração deve garantir a implementação dos princípios, políticas, estruturas organizacionais, processos e outros mecanismos necessários ao governo do Sistema de Informação.

3.2 O órgão de administração deverá nomear um «Comité estratégico/arquitetura do Sistema de Informação» ou função semelhante de suporte ao governo e gestão do Sistema de Informação.

3.3 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.

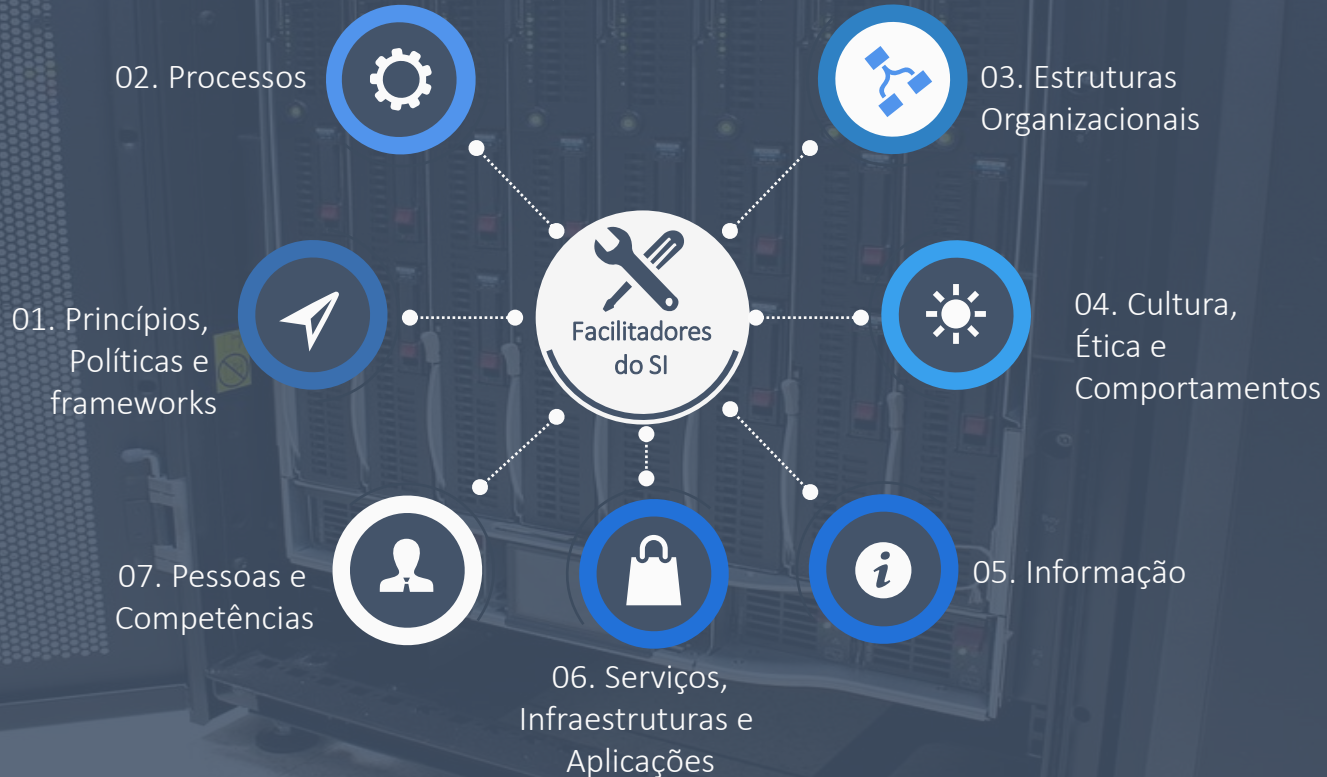
P#3

Organização



P#4 - Capacitação

6 Princípios e 22 Recomendações



Recomendações

4.1 O órgão de administração deve garantir 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.

4.2 O órgão de administração deve garantir a protecção da propriedade intelectual e a gestão do conhecimento relacionadas com o Sistema de Informação.

4.3 O órgão de administração deve garantir a revisão periódica e independente do governo e gestão dos serviços externos relacionados com o Sistema de Informação

P#4

Capacitação



P#5 – Risco e Conformidade

6 Princípios e 22 Recomendações



Recomendações

5.1 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.

5.2 O órgão de administração deve garantir a conformidade do Sistema de Informação com requisitos legais, normativos, contratuais e boas práticas de referência.

5.3 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.

5.4 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.

5.5 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.

P#5

Risco e
Conformidade



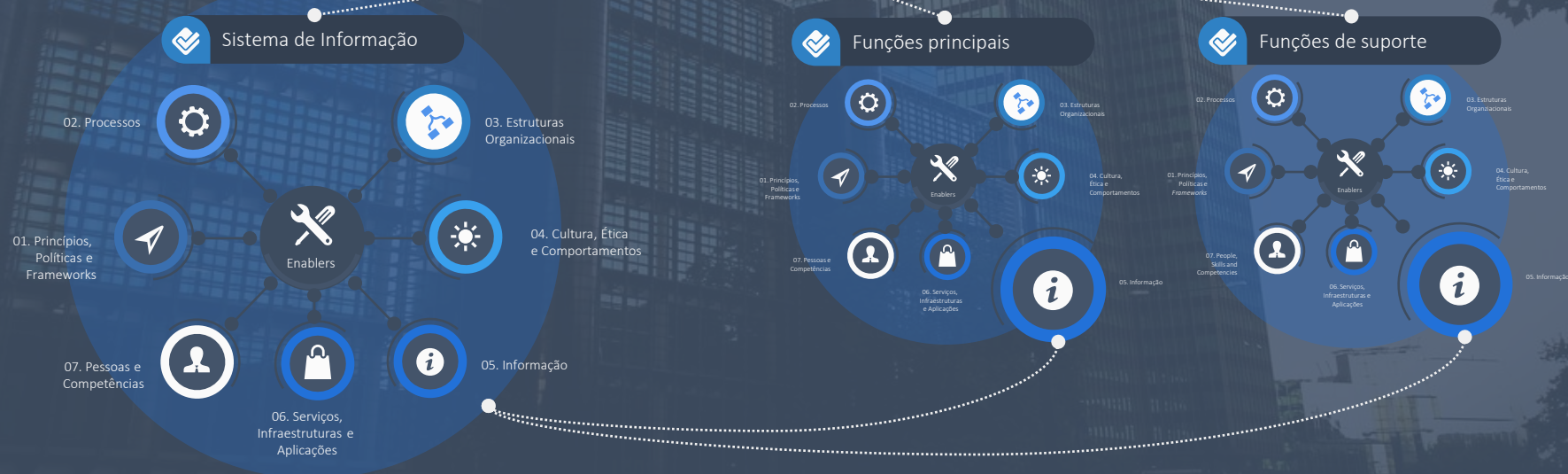
P#6 - Informação

6 Princípios e 22 Recomendações

Necessidades dos *stakeholders*



Objectivos corporativos



Recomendações

6.1 O órgão de administração deve garantir a definição e implementação de práticas de gestão que garantam a qualidade da Informação ao longo do seu ciclo de vida, nomeadamente em áreas como a «privacidade e protecção dos dados», «segurança da informação» ou «gestão do conhecimento».

6.2 O órgão de administração deve garantir que toda a Informação pessoal está identificada e é tratada como um activo importante da sociedade.

6.3 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.

P#6

Informação



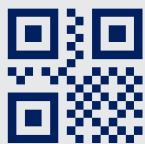


- ✗ “Foi um bug informático!”; “A culpa foi do informático!”; “A culpa foi do fornecedor!”
- ✓ Reconhecer a importância da Informação para a criação de valor na Organização
- ✓ “Será que estamos a fazer as coisas certas no Sistema de Informação? Será que estamos a ter os benefícios esperados?”
- ✓ Garantir o bom governo do Sistema de Informação : Avaliando, Dirigindo e Controlando.
- ✓ Garantir que o Governo do Sistema de Informação é parte integrante do Governo Societário.
- ✓ Adoptar as boas práticas de referência na Governança e Gestão do Sistema de Informação pode ser um factor crítico de sucesso (COSO, COBIT 5, ISO 38500...)



“There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know.”

Donald Rumsfeld



Download do documento

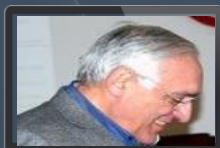
A “Proposta de princípios e recomendações para o governo societário de Sistemas de Informação” estará em consulta pública para análise e recolha de contributos.

Mais informação em www.cgov.pt



Até 31 de Julho de 2015

Grupo de Trabalho



Prof. Almiro de Oliveira, ISEG, UCP-Porto, Vice-Presidente e Fundador do ISGec/ceGSI, Presidente do ceGSI Portugal



(Coordenador)
Dr. Bruno Horta Soares, Senior Advisor em Governança e Gestão de Sistemas de Informação na GOVaaS e Presidente do ISACA Lisbon Chapter



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



Deloitte Portugal, representada por: Dr. João Carlos Frade e Eng.º Pedro Peralta



EY Portugal, representada por: Dr. Bruno Padinha



KPMG Portugal, representada por: Dr. Rui Gomes

Obrigado!



Autor: Bruno Horta Soares

IPCG

Edifício Victoria - Av. da Liberdade, n.º 196, 6.º andar, 1250-147 Lisboa 

(+351) 21 317 40 09 

ipcg@cgov.pt 