

Implementação e Administração de uma Política de Segurança

Vodafone Portugal

Orlando Fontan

IDC – IT & Internet Security – Centro Cultural de Belém
30.01.2007



Agenda

1. Gestão de Conformidades

Normas e Compliances (Basileia II, Sarbanes-Oxley e BS ISO/IEC 27001)

2. Estratégia de Segurança

Certificação BS ISO/IEC 27001

3. Gestão de Segurança nos casos de Outsourcing

Gestão de Contratos

Gestão de Recursos

4. Investimentos, custos e retorno

Gestão de Perfis de Acesso

Segregação de Funções

5. Caso Prático na Vodafone Portugal (Sessão da Tarde)

Gestão de Perfis de Acesso

Agenda

1. Gestão de Conformidades

Normas e Compliances (Basileia II, Sarbanes-Oxley e BS ISO/IEC 27001)

2. Estratégia de Segurança

Certificação BS ISO/IEC 27001

3. Gestão de Segurança nos casos de Outsourcing

Gestão de Contratos

Gestão de Recursos

4. Investimentos, custos e retorno

Gestão de Perfis de Acesso

Segregação de Funções

5. Caso Prático na Vodafone Portugal (Sessão da Tarde)

Gestão de Perfis de Acesso

Gestão de Conformidades

Normas e Compliances (Basileia II, Sarbanes-Oxley e BS ISO/IEC 27001)

Basileia II

- Necessidade dos bancos disporem de fundos próprios para fazer face ao Risco Operacional.
- Definição de requisitos mínimos de capital.
- Definição clara das responsabilidades das entidades supervisoras bancárias.
- Obrigação no fornecimento de informação quantitativa de risco aos investidores e ao mercado.
- Limitar a possibilidade de ocorrência de outra crise bancária internacional;
- Assegurar que cada banco, dispõe de níveis de capital suficientes para realizarem as actividades que compreendem algum risco.

Gestão de Conformidades

Normas e Compliances (Basileia II, Sarbanes-Oxley e BS ISO/IEC 27001)

Basileia II



Gestão de Conformidades

Normas e Compliances (Basileia II, Sarbanes-Oxley e BS ISO/IEC 27001)

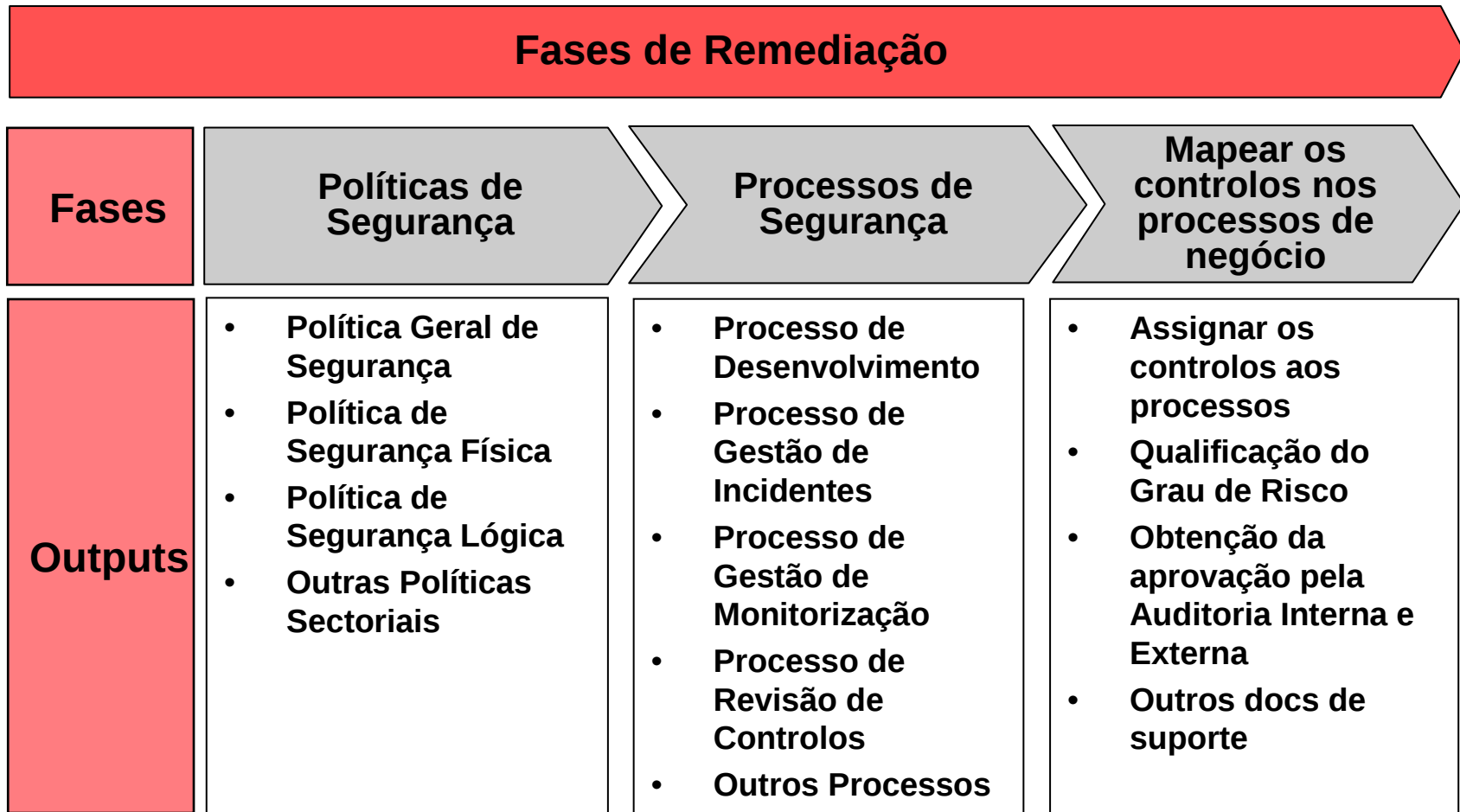
Sarbanes-Oxley (Sarbox ou Sox)

- Lei americana, assinada em 30 de julho de 2002, pelos senadores Paul Sarbanes (Democrata de Maryland) e Michael Oxley (Republicano de Ohio);
- Motivada por escândalos financeiros corporativos, (Enron, Worldcom, etc.);
- O principal objectivo de evitar a ocorrência de Fraude Financeira;
- Ter mecanismos de auditoria e segurança mais fiáveis;
- Criação de comités de auditoria, supervisão e monitorização;
- Acima de tudo Transparência.

Gestão de Conformidades

Normas e Compliances (Basileia II, Sarbanes-Oxley e BS ISO/IEC 27001)

Sarbanes-Oxley



Gestão de Conformidades

Normas e Compliances (Basileia II, Sarbanes-Oxley e BS ISO/IEC 27001)

BS ISO/IEC 27001:2005

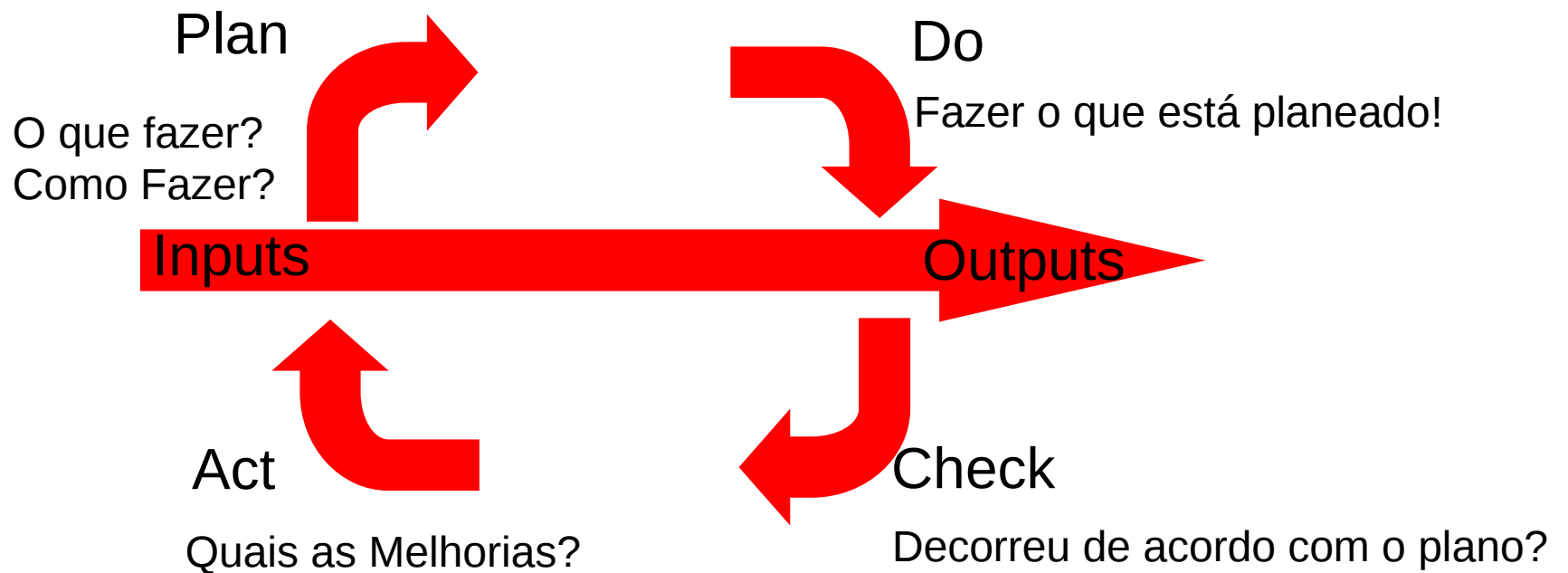
- Definição de exigências e objectivos da segurança;
- Assegura que os riscos da segurança são eficazmente geridos;
- Permite assegurar a conformidade com leis e regulamentos;
- Utilizada para implementação e gestão de controlos;
- Ajuda na definição de novos processos de gestão de segurança da informação;
- Identifica e clarifica os processos existentes de gestão da segurança da informação;
- Pode ser utilizada auditores internos e externos, na determinação do grau de conformidade com políticas, directrizes, normas e procedimentos adoptados pela organização;
- Permite à organização fornecer informação sobre políticas e procedimentos de segurança da informação, por razões operacionais ou comerciais;

Gestão de Conformidades

Normas e Compliances (Basileia II, Sarbanes-Oxley e BS ISO/IEC 27001)

BS ISO/IEC 27001:2005

- Permite certificar um sistema de gestão de segurança da informação (Information Security Management System - ISMS);
- Esta norma tem origem na norma BS 7799-2 e encontra-se alinhada com o modelo PDCA (Plan-Do-Check-Act).



Gestão de Conformidades

Curiosidades

Desenrascanço

- Desenrascanço is a Portuguese word used, in common language, to express an ability to solve a problem without having the knowledge or the adequate tools to do so, by use of imaginative resources or by applying knowledge to new situations. [...]
- Achieved when resulting in a hypothetical good-enough solution. When that good solution doesn't occur we got a failure (enrascanço). [...]
- Desenrascanço, in fact, is the opposite of planning, but managing for the problem not becoming completely out of control and without solution.[...]

Fonte: Wikipedia

"Em momentos de crise, a imaginação é mais importante que o conhecimento."
Albert Einstein

Alteração de mentalidades !!! (Norte da Europa/ Sul da Europa)

Agenda

1. Gestão de Conformidades

Normas e Compliances (Basileia II, Sarbanes-Oxley e BS ISO/IEC 27001)

2. Estratégia de Segurança

Certificação BS ISO/IEC 27001

3. Gestão de Segurança nos casos de Outsourcing

Gestão de Contratos

Gestão de Recursos

4. Investimentos, custos e retorno

Gestão de Perfis de Acesso

Segregação de Funções

5. Caso Prático na Vodafone Portugal (Sessão da Tarde)

Gestão de Perfis de Acesso

Estratégia de Segurança

Certificação BS ISO/IEC 27001)



Agenda

1. Gestão de Conformidades

Normas e Compliances (Basileia II, Sarbanes-Oxley e BS ISO/IEC 27001)

2. Estratégia de Segurança

Certificação BS ISO/IEC 27001

3. Gestão de Segurança nos casos de Outsourcing

Gestão de Contratos

Gestão de Recursos

4. Investimentos, custos e retorno

Gestão de Perfis de Acesso

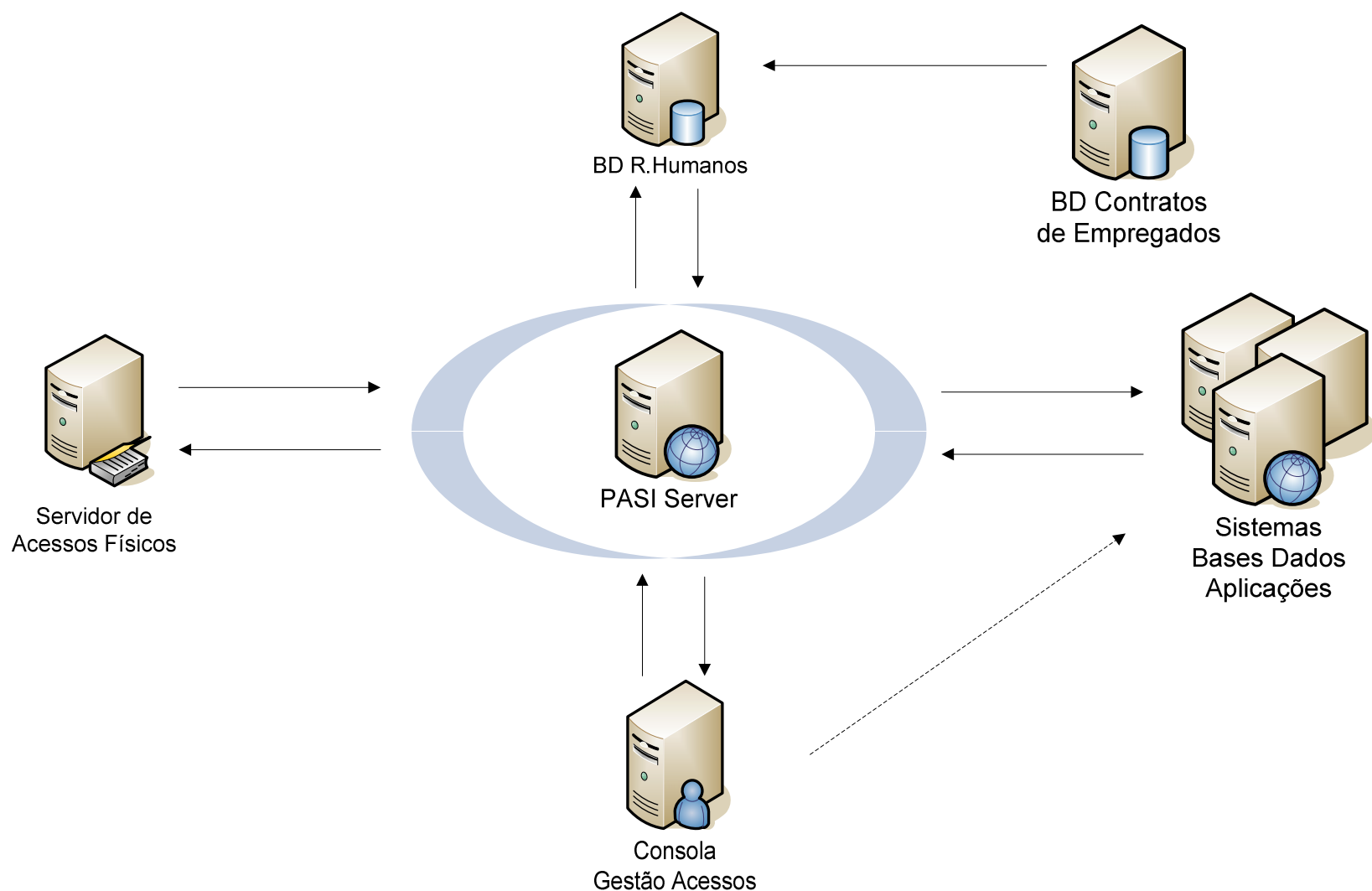
Segregação de Funções

5. Caso Prático na Vodafone Portugal (Sessão da Tarde)

Gestão de Perfis de Acesso

Gestão de Segurança nos casos de outsourcing

Desenho do Sistema



Agenda

1. Gestão de Conformidades

Normas e Compliances (Basileia II, Sarbanes-Oxley e BS ISO/IEC 27001)

2. Estratégia de Segurança

Certificação BS ISO/IEC 27001

3. Gestão de Segurança nos casos de Outsourcing

Gestão de Contratos

Gestão de Recursos

4. Investimentos, custos e retorno

Gestão de Perfis de Acesso

Segregação de Funções

5. Caso Prático na Vodafone Portugal (Sessão da Tarde)

Gestão de Perfis de Acesso

Investimento, custos e retorno

Factos que falam por si



Equipa de 4 elementos

+650 Logins de Sistemas
(BD, SO e APP)



+3.500 Colaboradores
(Internos + Outsourcing)

Ganhos significativos de
produtividade / custos





VF-PT Corporate Security & BCM

Orlando Fontan
(orlando.fontan@vodafone.com)

Obrigado!