

Disaster Recovery Plan (DRP)

Lucas Ribeiro, C.H.T.M.A.D, EPE
lucas@chtmad.min-saude.pt

Agenda



- Parte 1 - A segurança nos Hospitais Portugueses:
 - **A importância da segurança;**
 - **Resultados relativos à segurança** (abrangência ARS Norte)
Information systems heterogeneity and interoperability inside hospitals – a survey;
- Parte 2 - *Disaster Recovery Plan (DRP)*:
 - Introdução;
 - Importância do DRP;
 - Metodologia;
 - Desenvolvimento do DRP;
 - DRP no CHTMAD.



Importância da segurança

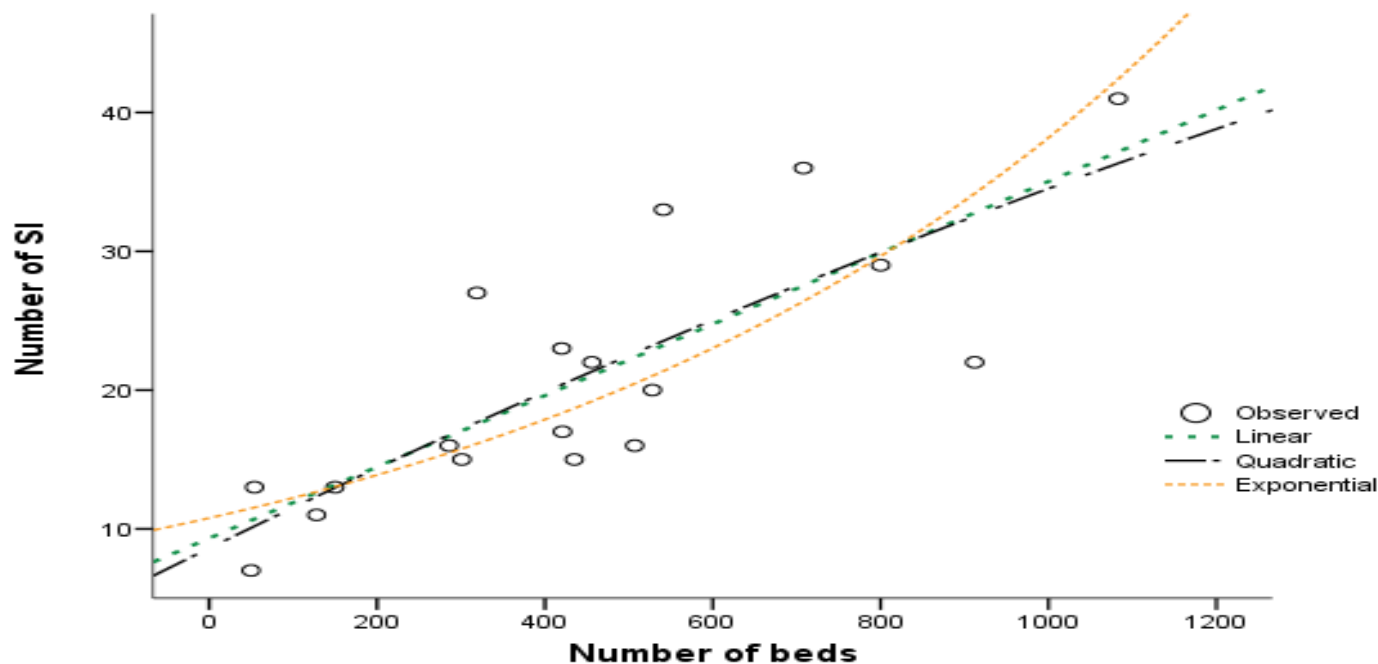


- Num ambiente hospitalar, o que é mais preocupante?
 - Informação clínica dos doentes (histórias clínicas, prescrições, resultados laboratoriais, imagem, etc);
 - O que não é importante?
- **Características da segurança:**
 - **Confidencialidade;**
 - **Disponibilidade;**
 - **Integridade.**



Resultados (segurança)

ARS Norte - 18 Organizações (34 hospitais)



$$N_{SI} = 10,78 e^{0,001 N_{Camas}}$$

Exponencial ($R^2=0,65$)

Linear ($R^2=0,64$); Quadrático ($R^2=0,64$)

Resultados (segurança)

Tipos de SI	Instalações SI		Diferentes SI		Rácio
	N	%	N	%	
Globais (ADT ou EPR)	67	16	8		8.4
Departamentais	349	84	119		2.9
SI Laboratórios	58	14	22		2.6
Imagiologia (RIS e PACS)	41	10	17		2.4
Prescrição e dispensa de medicamentos	34	8	6		5.7
Outros	216	52	74		2.9
Total:	416		127		3.3

Média de SI por organização (apenas SI clínicos) = 21

Discussão



- Considerando que:
 - Apenas analisamos SI clínicos;
 - Restantes SI são consideráveis (ERP, por exemplo);
 - Não consideramos as Infra-estruturas de suporte (AD, DNS, DHCP, etc);
- Problemas na segurança:
 - Grande número de SI;
 - Alguns deles obsoletos...
 - Enorme heterogeneidade;
 - Integrações – indisponibilidade de uns condiciona a disponibilidade de outros.

Como garantir a segurança nestas condições?



DRP - Introdução

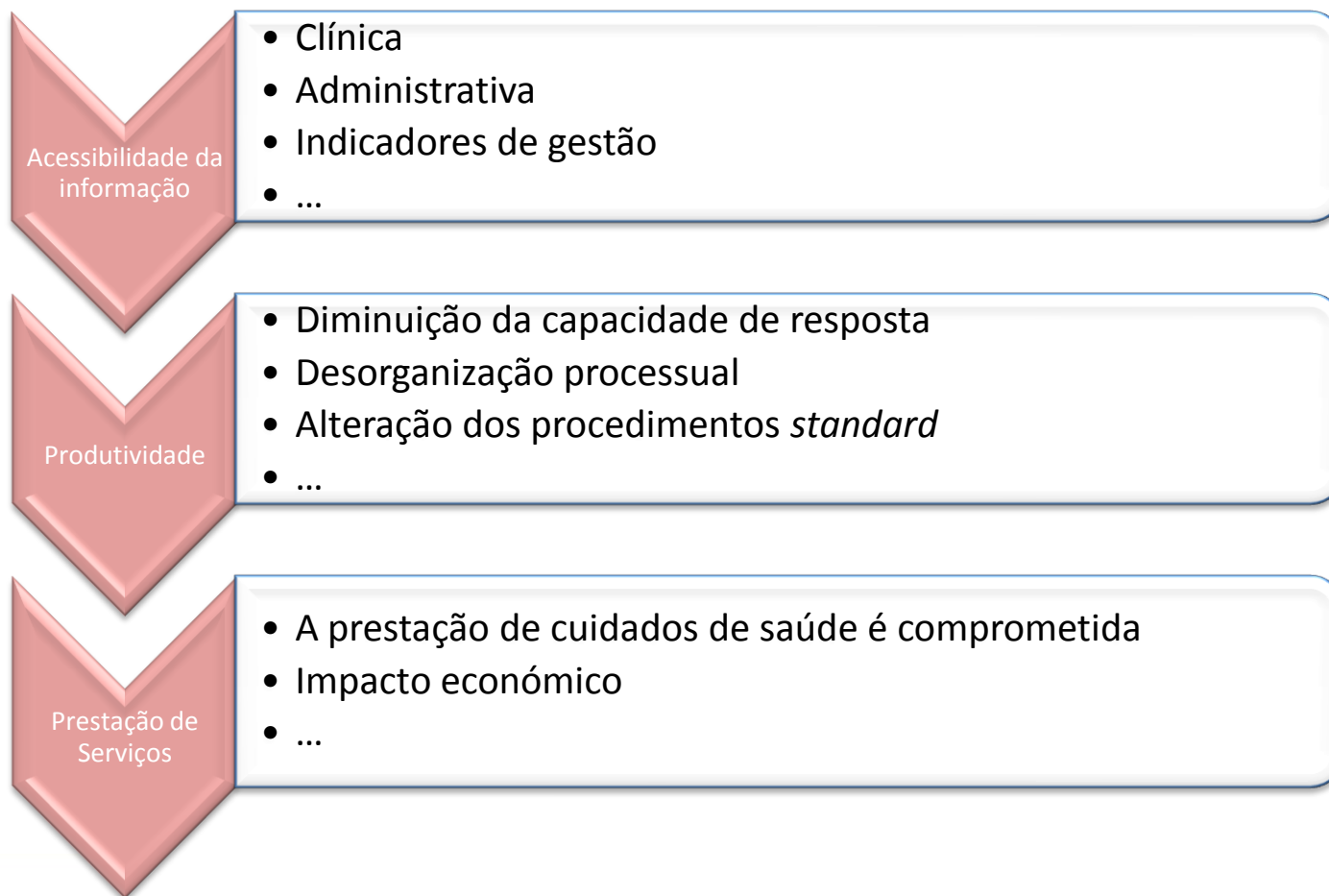
Qual o impacto de falhas nos Sistemas de Informação?

Quem está imune a falhas?



DRP - Introdução

Impacto de falhas nos Sistemas de Informação no *negócio* da organização



DRP - Introdução



- Incidentes previsíveis e imprevisíveis podem ocorrer e ocorrem sistematicamente, de facto, no âmbito dos sistemas de informação.
- Para a organização sobreviver a um desastre neste âmbito, necessita de recuperar desses desastres.
- **DRP: Um plano que sistematiza as acções e decisões a desenvolver e efectuar, tendo em conta os objectivos de recuperar:**
 - **O mais rapidamente possível**
 - **Com o mínimo de danos**
 - **Com o custo mínimo**
 - **Com o mínimo de impacto nos utilizadores e utentes**



DRP - Introdução



Torna-se assim necessário . . .

- Definir os sistemas vitais à continuidade de operação da organização;
- Alinhamento completo com Administração e Direcções de Processos Críticos;
- Conhecimento profundo da realidade IT e sua integração nos processos de negócio;
- **Estar preparado para o desastre (independentemente da gravidade).**

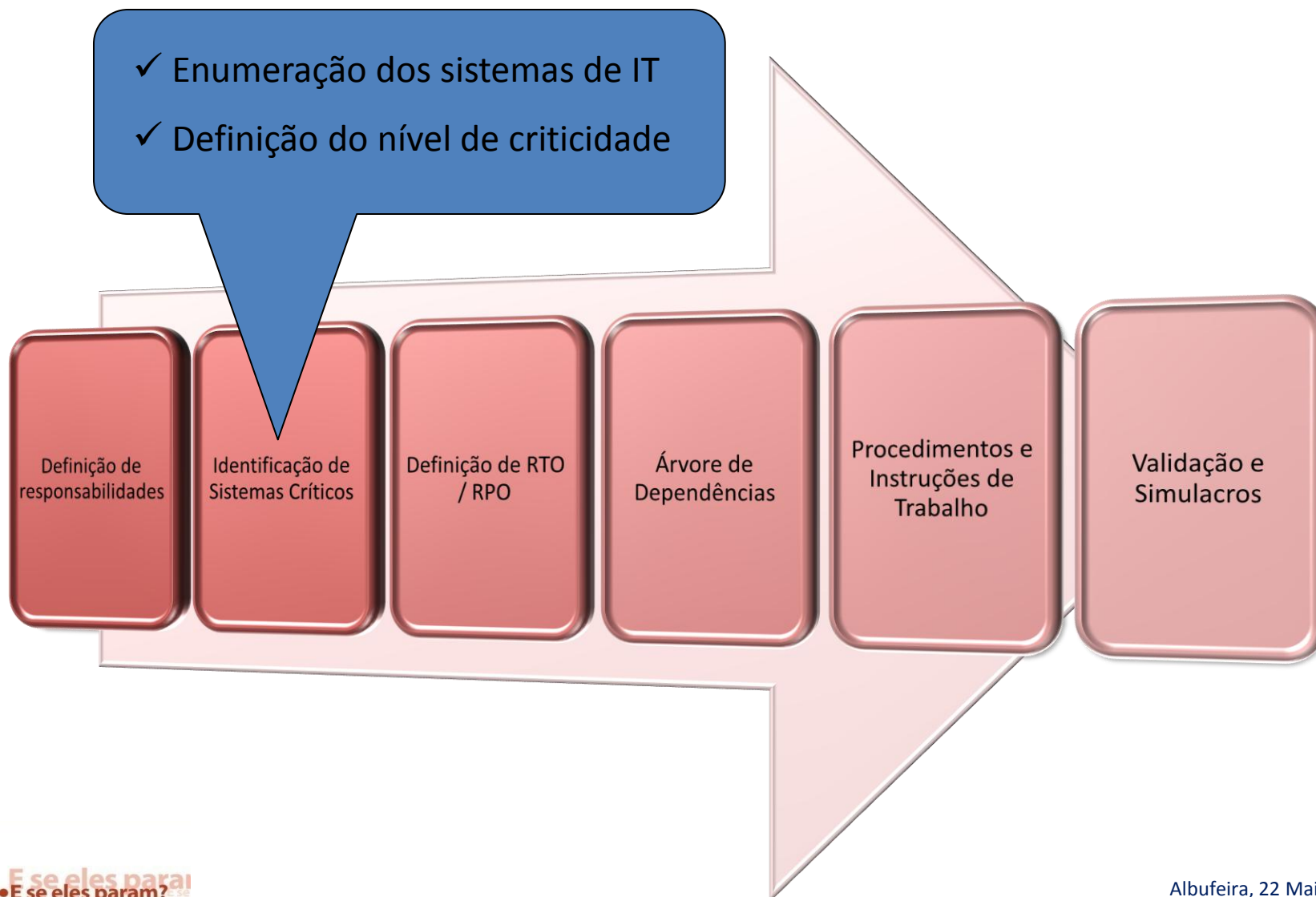


DRP - Metodologia

- ✓ Identificação da responsabilidade de definição do plano
- ✓ Identificação da responsabilidade de activação do plano
- ✓ Identificação da responsabilidade de manutenção do plano
- ✓ Identificação de meios de comunicação

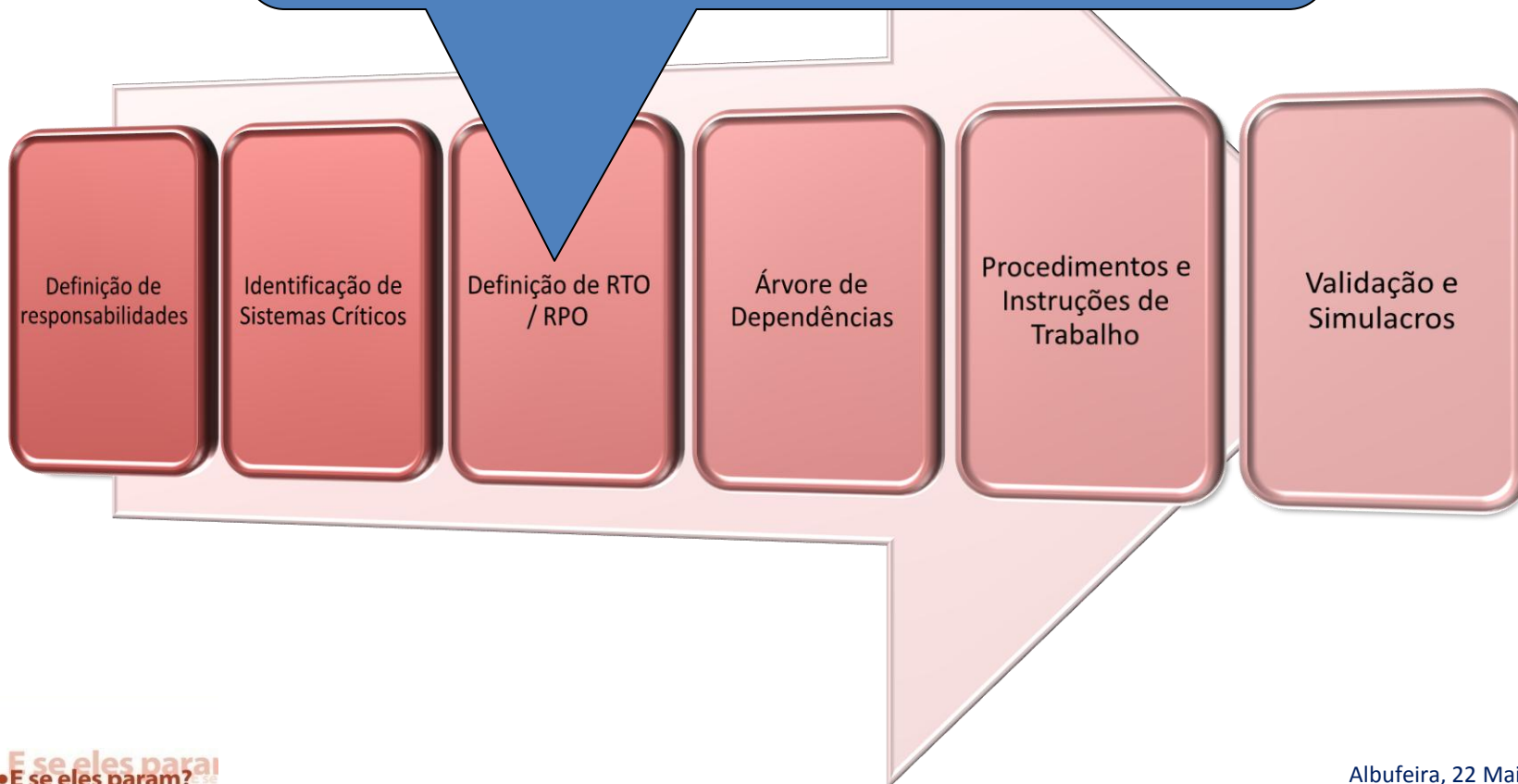


DRP - Metodologia



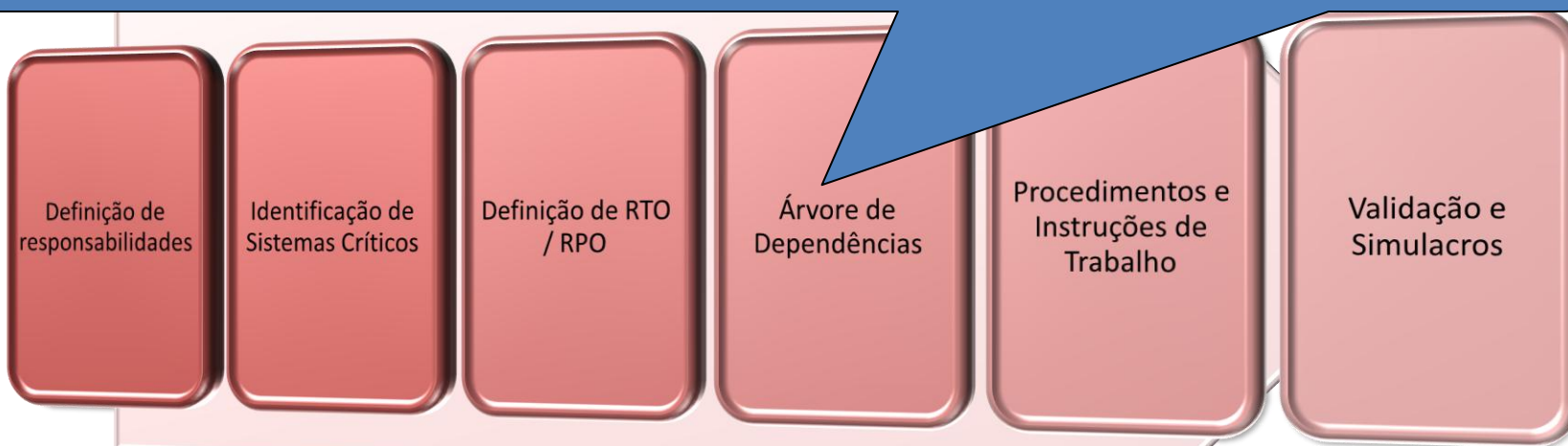
DRP - Metodologia

- ✓ Definição dos objectivos de tempos de recuperação
- ✓ Definição das perdas máximas de dados



DRP - Metodologia

- ✓ Caracterização de objectos
- ✓ Identificação de dependências entre serviços e entre camadas (HW, SW, Aplicações)
- ✓ Caracterização de dependências



DRP - Metodologia

- ✓ Procedimentos de Salvaguarda de dados, aplicações e sistemas
- ✓ Procedimentos de recuperação de dados, aplicações e sistemas
- ✓ Informações sobre terceiros necessários à efectivação de procedimentos

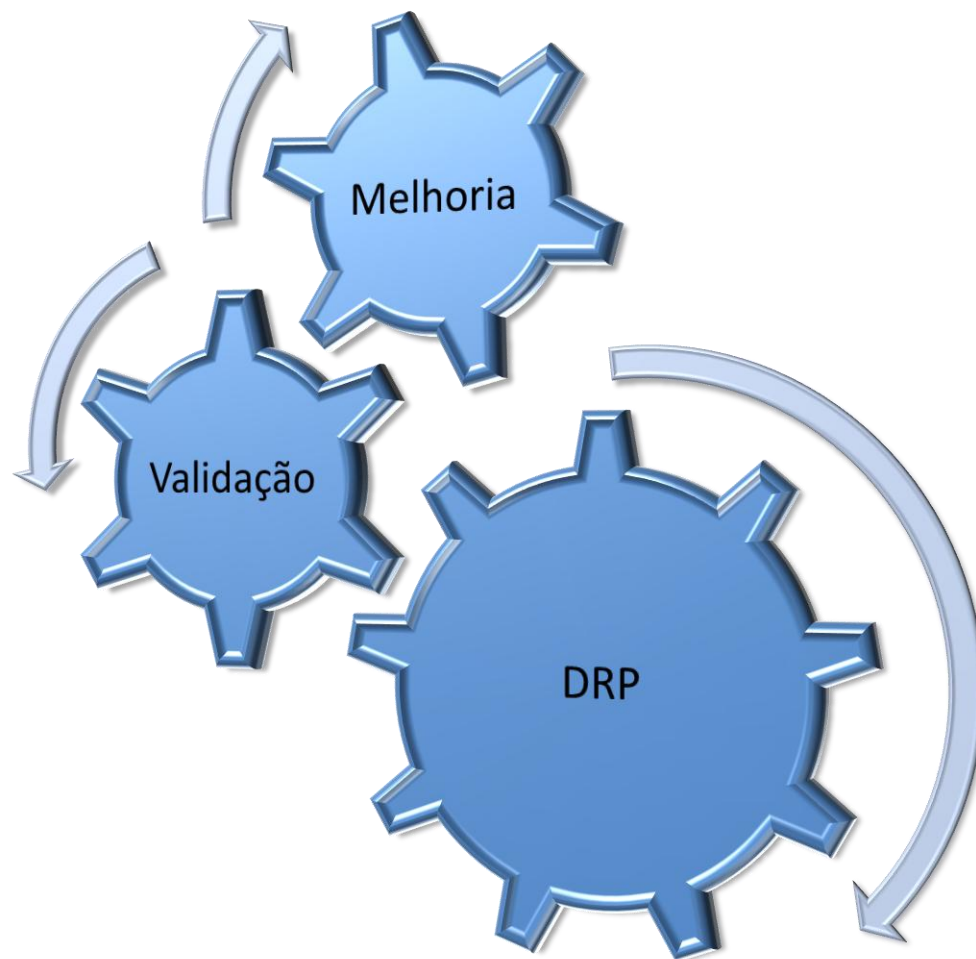


DRP - Metodologia

- ✓ Definição de métodos de validação de capacidade de recuperação de desastres
- ✓ Efectivação de simulacros
- ✓ Identificação de riscos
- ✓ Obtenção de dados para ciclo de melhoria do DRP



DRP - Melhoria contínua



DRP - Melhoria contínua



Prestação de Serviços IT de
encontro ao negócio

DRP - CHTMAD



- Plano iniciado há cerca de um ano;
 - 1ª Etapa – Identificação de todos os SI;
 - 2ª Etapa – Mecanismos de backup;
 - ...
 - Conclusão 1º semestre de 2010;
- Processo evolutivo:
 - Ganhos em cada etapa;
- Documento de fácil leitura e pragmático;
- Processo de identificação de riscos / Mitigação de riscos;
- Melhorar tempos de recuperação;
- Processo contínuo de melhoria.



Disaster Recovery Plan (DRP)

Obrigado pela atenção!

Lucas Ribeiro, C.H.T.M.A.D, EPE
lucas@chtmad.min-saude.pt