Pan Rio 2007
Implementação de Segurança da Informação

Entalpia Security

Reinaldo de Medeiros

Agenda

- Singularidade Metodologia e Arquitetura
- Gerenciamento de Risco
- *Hardening*
- *Análise de Risco*
- Análise de Vulnerabilidade
- Monitoramento SIEM
- Os “Ensaios Técnicos”
- Legado – Erros e Acertos

Pan Rio 2007

- 46 instalações
- 15.000 voluntários
- 3.000 jornalistas
- 5.634 atletas de 42 países
- 330 competições
- 34 esportes
- 2.211 medalhas

Desafios

- Alta visibilidade e criticidade
- Prazo fixo – Sem segunda chance
- Gerenciamento de Projetos Complexos
- Grande quantidade *players* envolvidos
- Torre de Babel
- Equipe especializada
- 30 sistemas integrados
- Visibilidade Global

Visibilidade Global

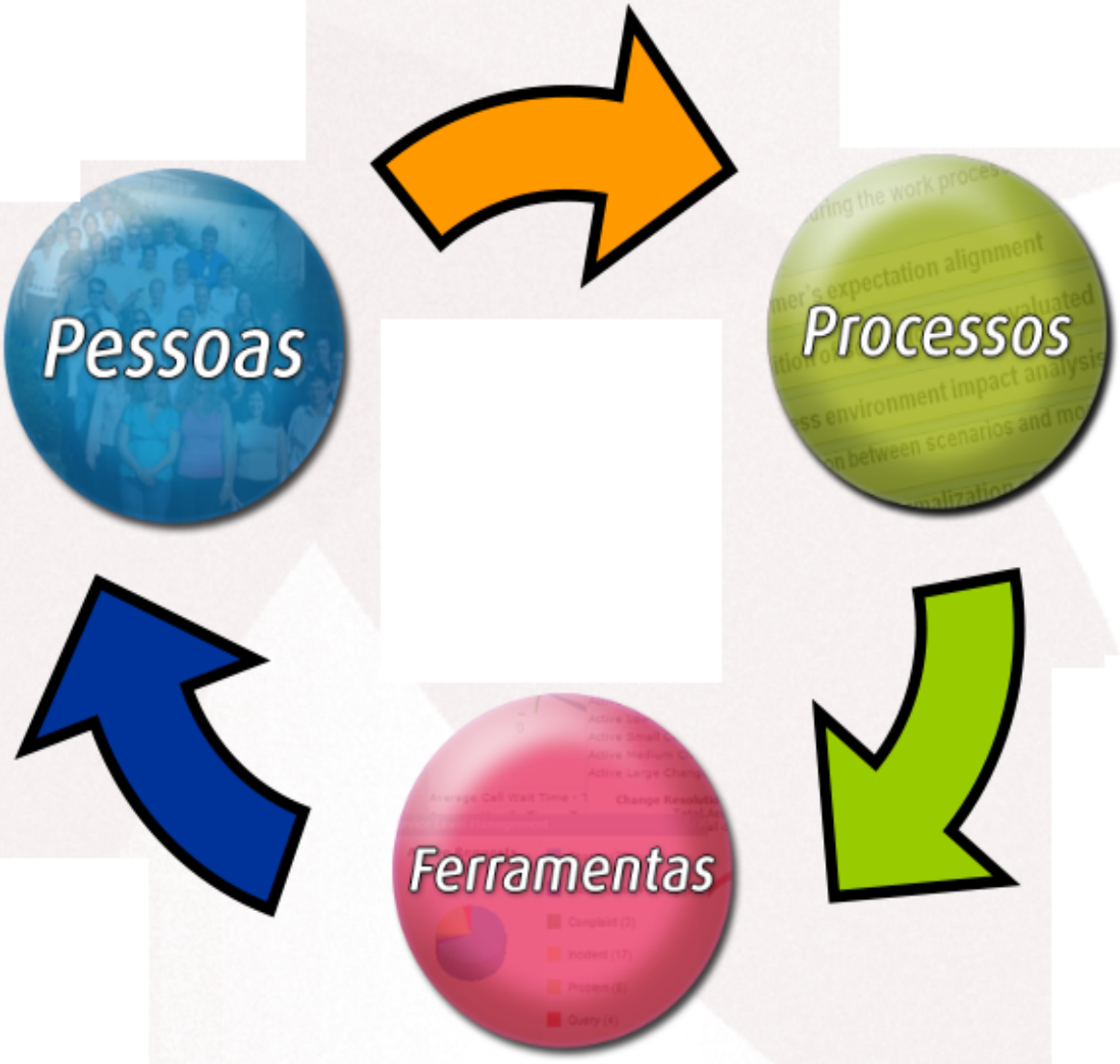
Atlanta - 96

- Exercício Prático
- Busque no Google:
  - IBM Atlanta Oly...
- Qual a sugestão do autocompletar?

Template Atos - Singularidade

- Barcelona 92
- Parceria com o CO desde 2001
- Aprendizado Contínuo nos Diversos Jogos
- Gestão Integrada Entre Todos os Serviços

Metodologia

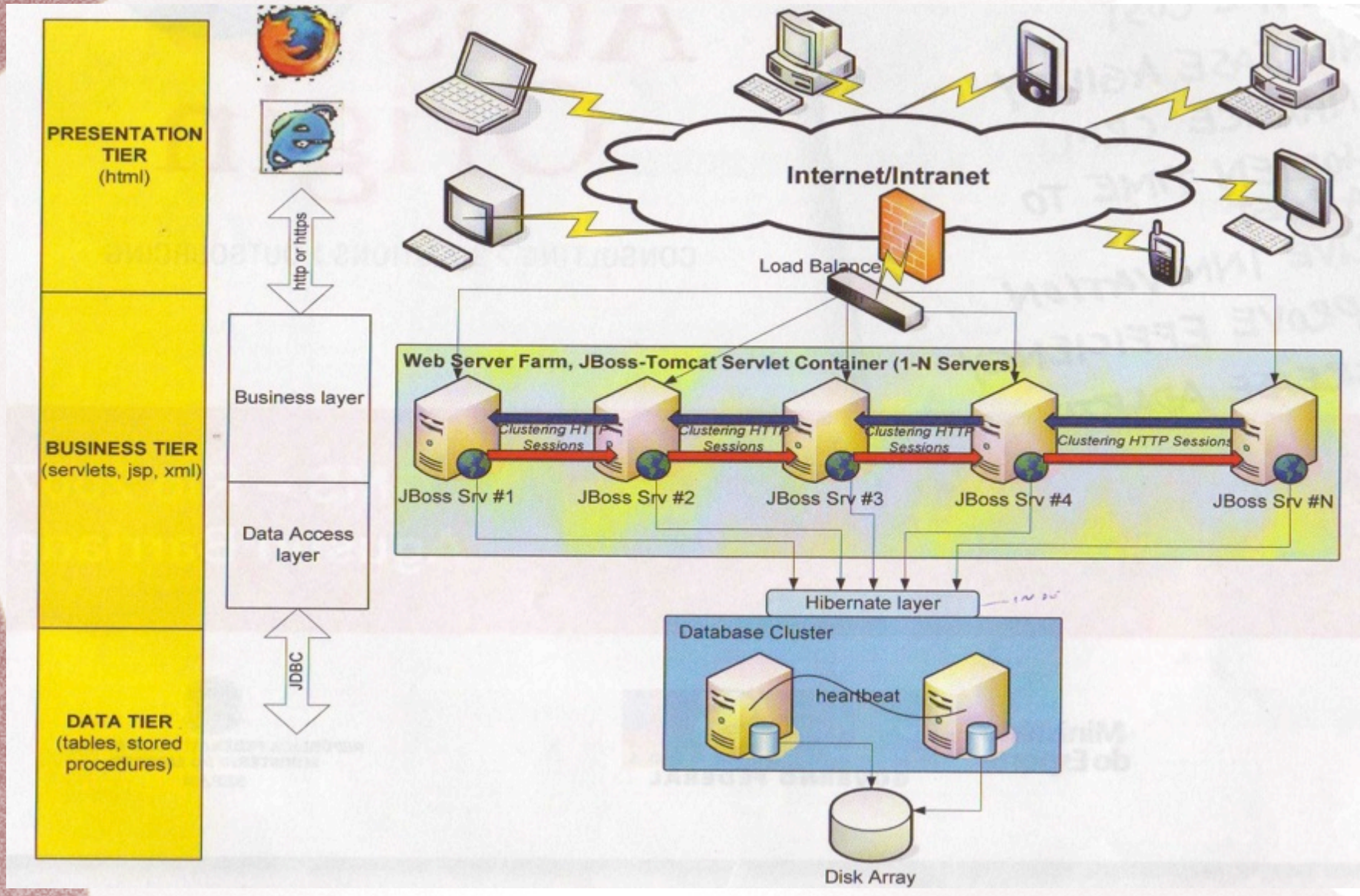


Sistemas Maduros

Sistemas Corporativos

RFID

Arquitetura de Sistemas



Documentação

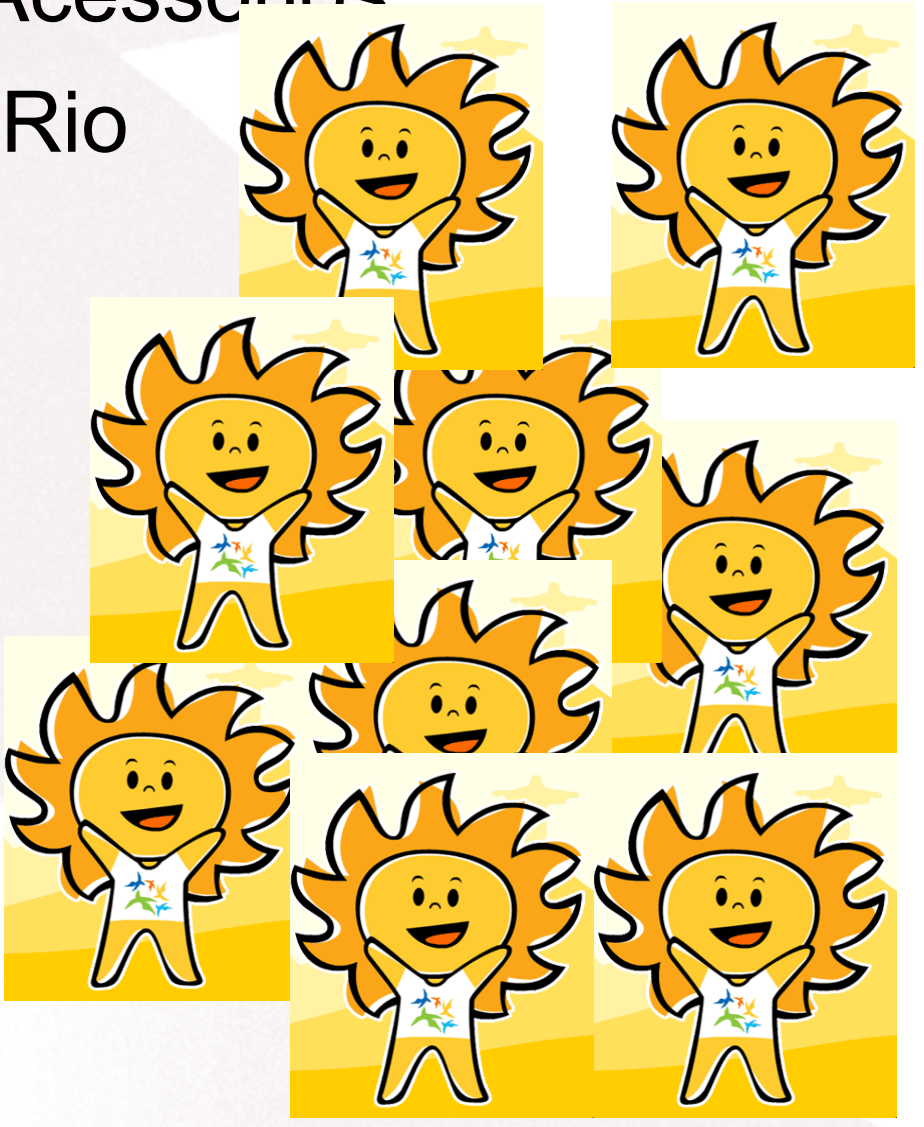
- *Template* bem definido e seguido por todos
- Todos os sistemas e procedimentos devidamente documentados
- Nada funcionaria sem procedimento
- Equipes diferentes implementavam

Pressão por prazos

- Baixa tolerância à falhas ou ineficiências
- Turnover Considerável
  - Documentação
- Adrenalina
- 'Plano B' Pra quase tudo

Equipe Inicial – Dez/06

- Windows e Seus Acessórios
- Service Desk - CoRio
- Portais e Intranet
- Bancos de Dados
- Aplicações
- Redes
- Segurança
- +ou- 20 pessoas



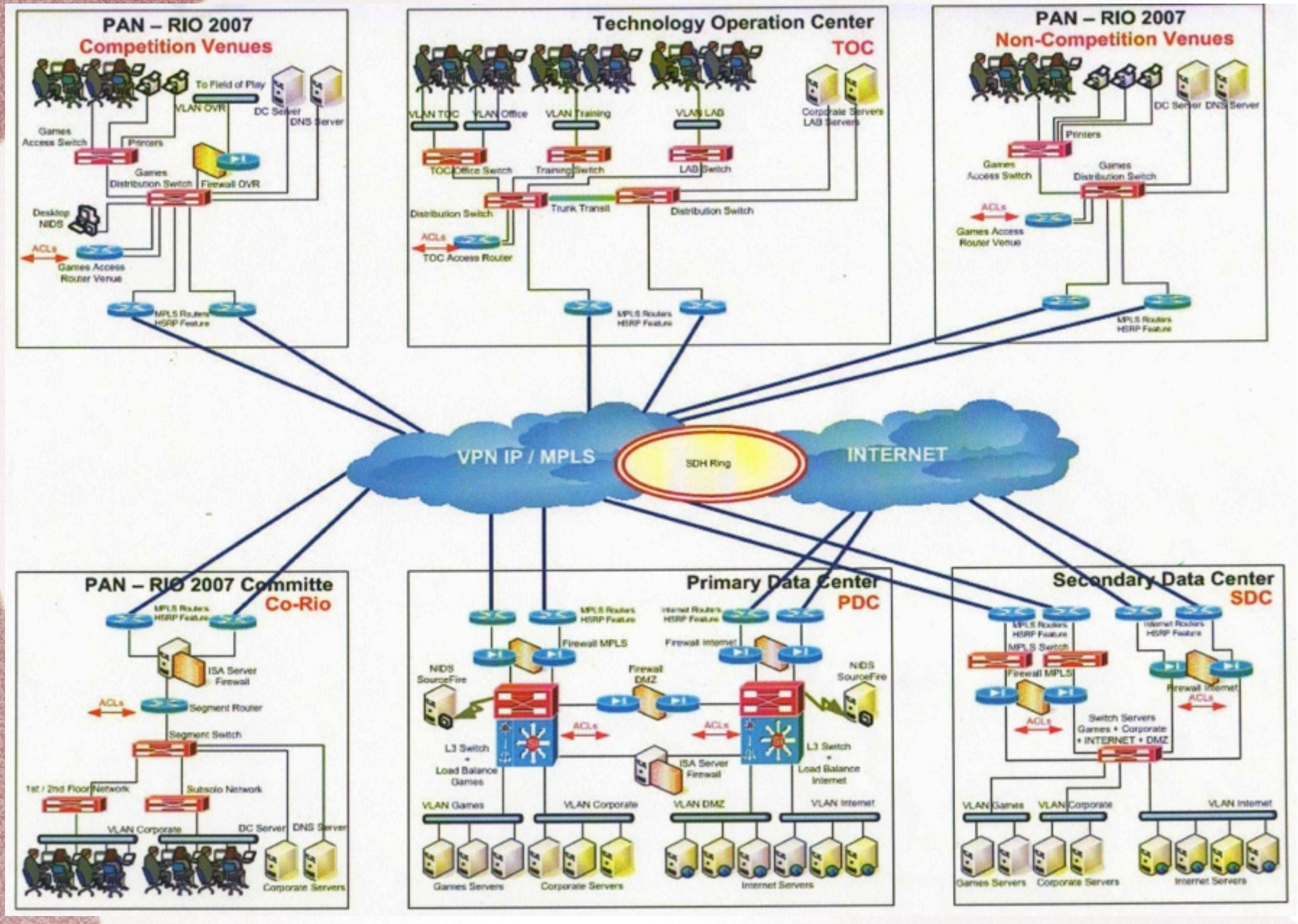
Equipe de Segurança - Interoperável

- Coordenador Arquitetura de Solução
  Luciano Wulff
- Implementação e Operação
  Kenia Gaipo -> Ivan Aquino
- Monitoramento e Incidentes
- Riscos e Vulnerabilidades
  Reinaldo Medeiros

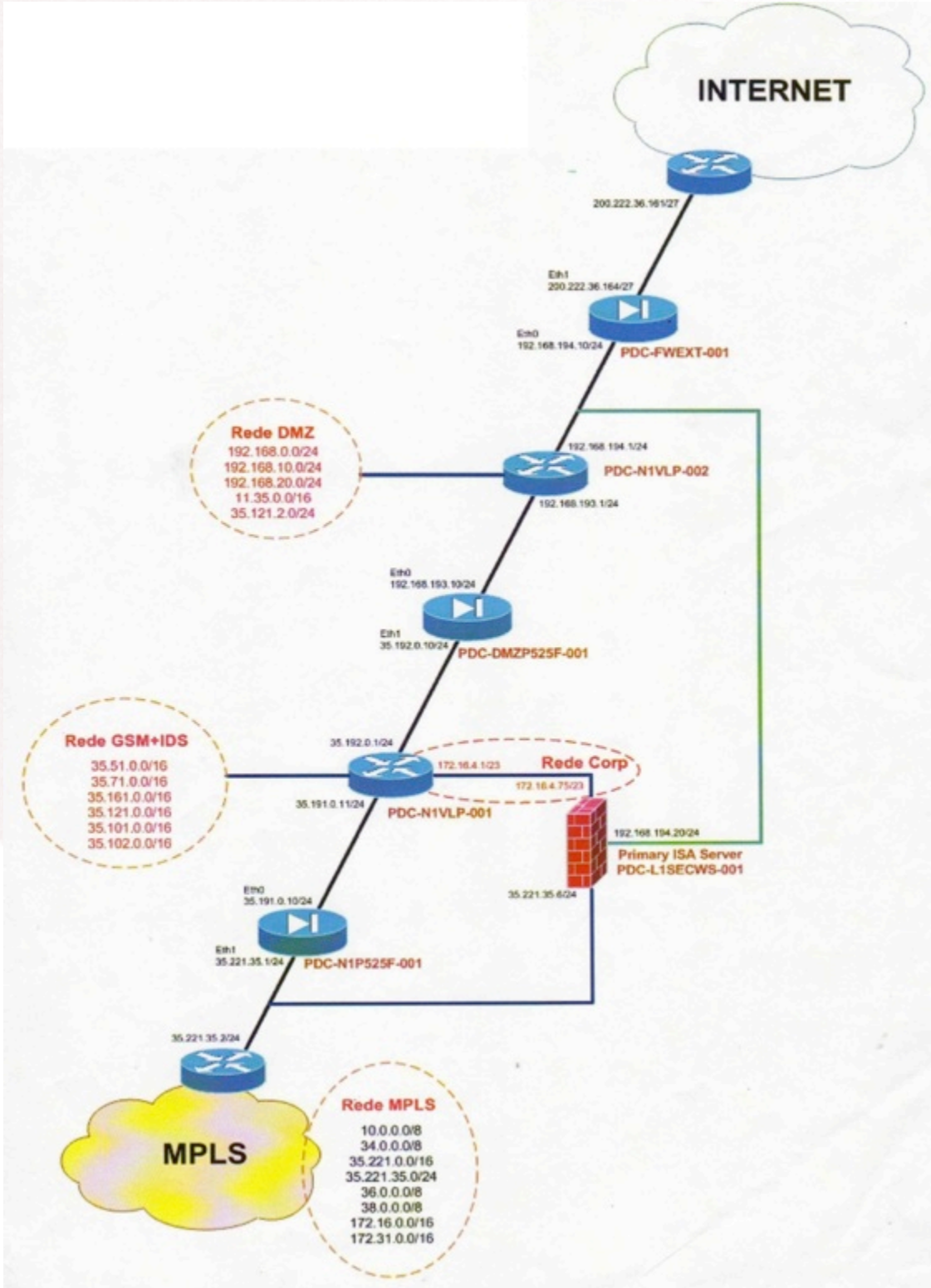
Infraestrutura
“E Fez-se Luz”

- Deus criou o mundo em 7 dias porque não havia usuário, base instalada e nem legado
- Desenhada do Zero
- *Hardware* e *software* padronizados
- Até infraestrutura *Windows* funciona bem...

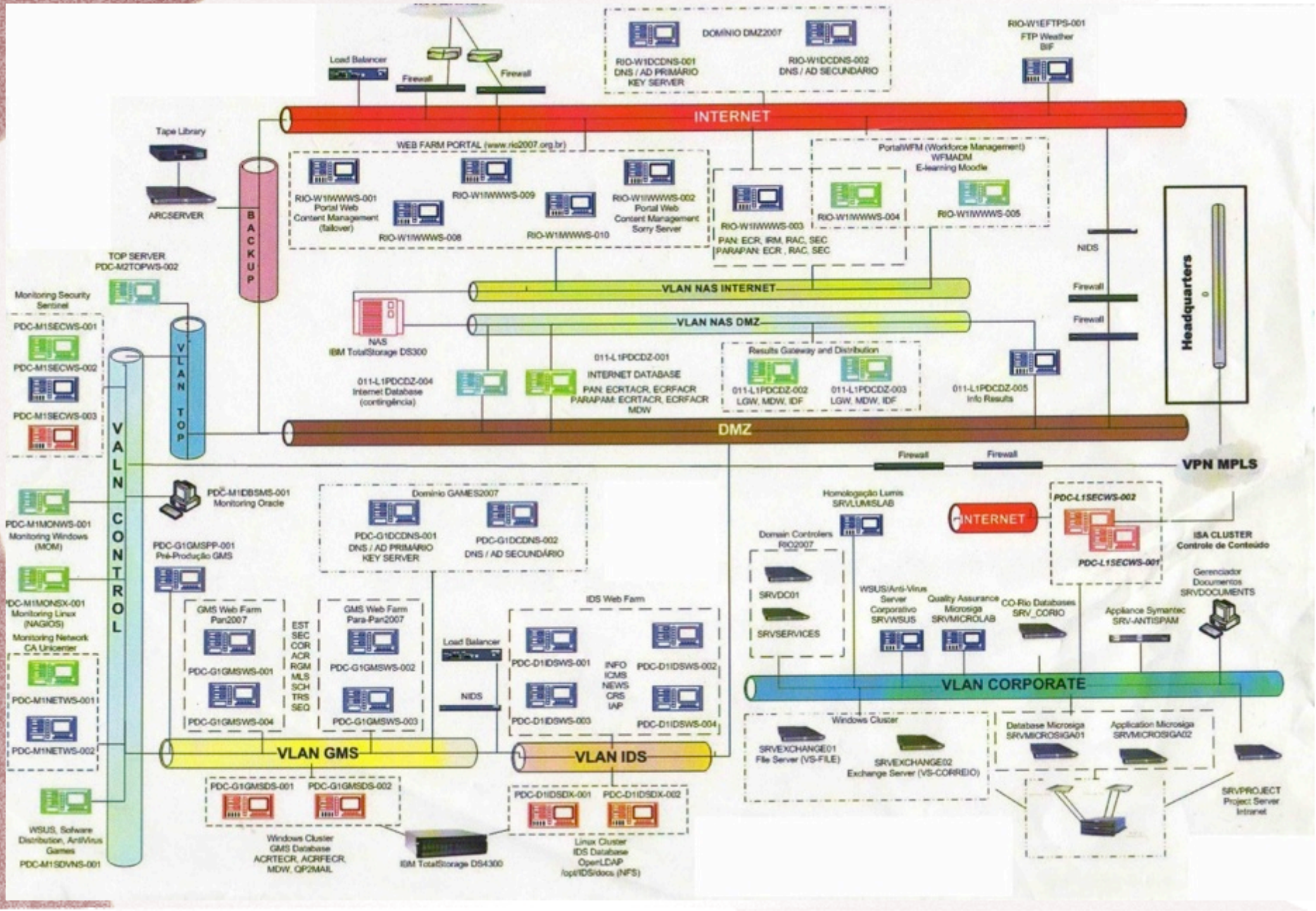
Arquitetura Física



Firewalls - Posicionamento



Detalhadamente...



Infra Básica de InfoSec

- Antivírus
- Filtro Web
- AD
- WSUS
- ISA
- Sourcefire*
- Cisco PIX

Open Source

Snort

Nagios

Nessus*

Treinamento Corporativo

- Desafio Abissal
- Níveis Diferentes
  - TI, Corporativo, Voluntários
- Tempo Exíguo
- Foco no básico
  - Uso de Internet e Recursos.
  - Controle de Acessos
  - Riscos

Estrutura de Contingência

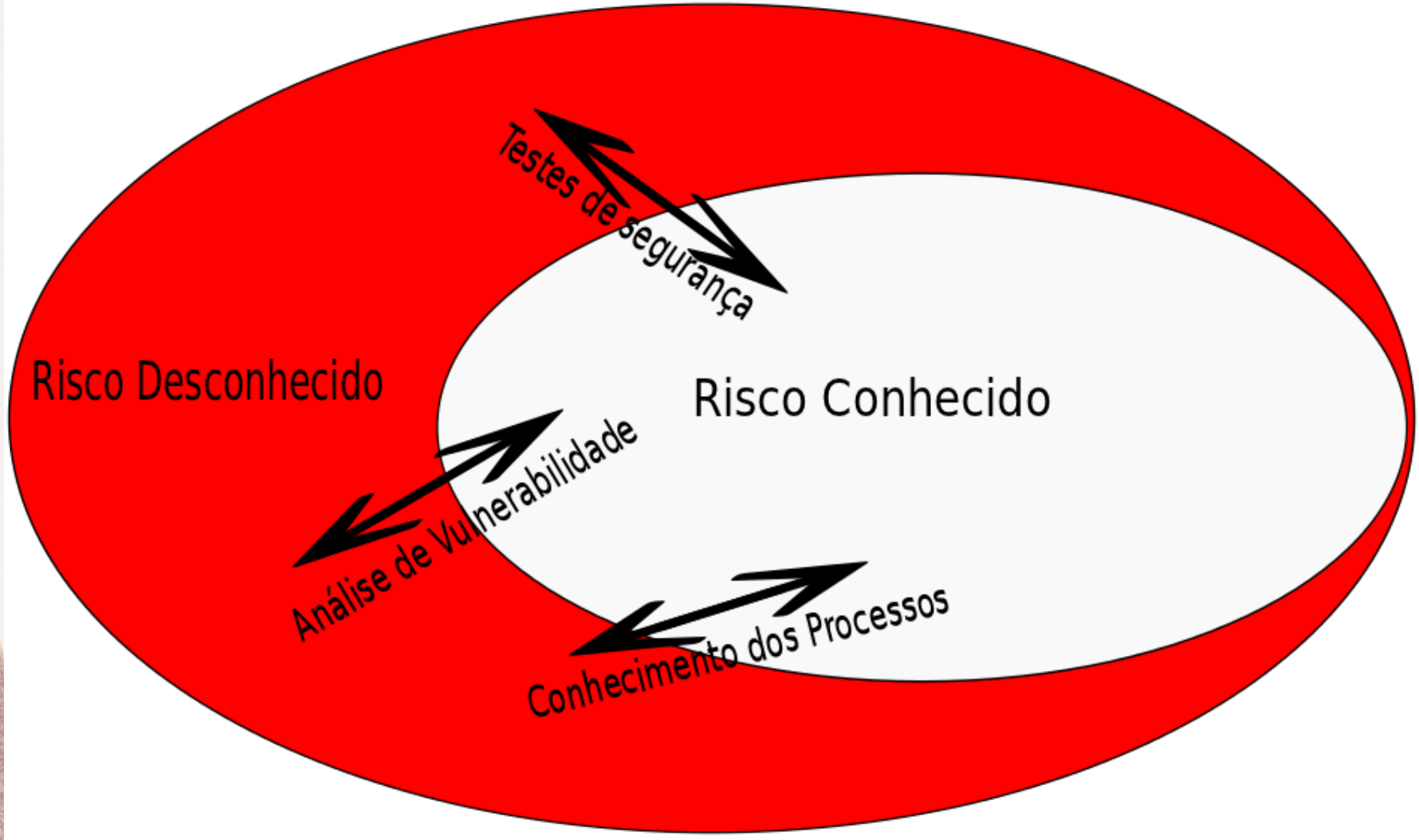
- Links e Data Center reserva
  - Com Servidores e Aplicações
  - Gente e Procedimento
  - Para-Pan
- Localização Geográfica
  - PDC - Botafogo
  - SDC - Cittá (Barra – A Miami que deu errado)
- Testes de Contingência


ALOG DATACENTERS - Unidade RJ
Citta América
Gray Buildings © 2008 Sanborn
Image © 2012 GeoEye
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
Google

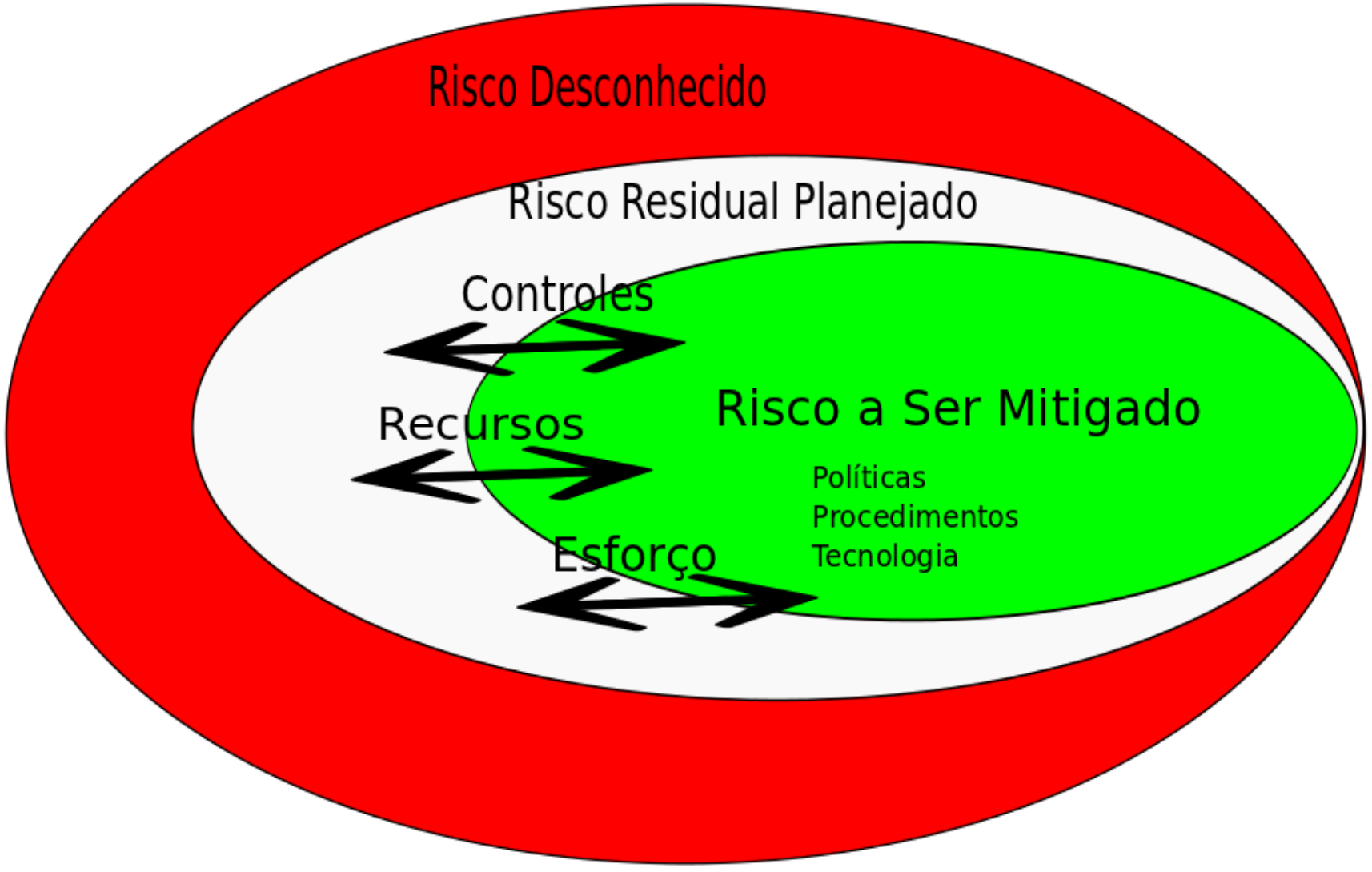
Gerenciamento de Risco

- Procedimento desenvolvido pela *Schlumberger*
- Ofertas de Mercado
  - Risco Desconhecido
- Software GRC escolhido: Excel

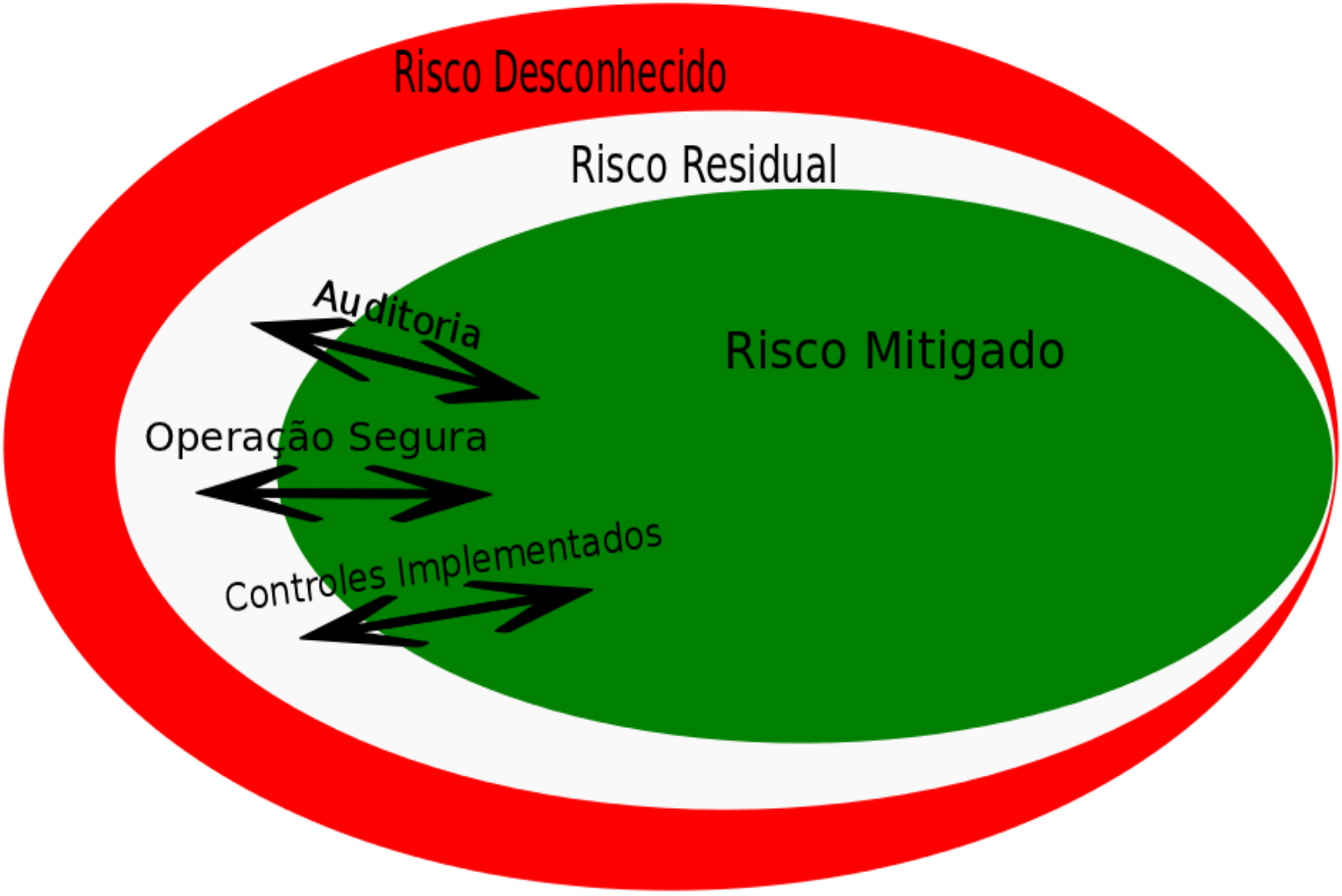
Risco Desconhecido vs Conhecido



Risco Mitigado



Gerenciamento de Risco

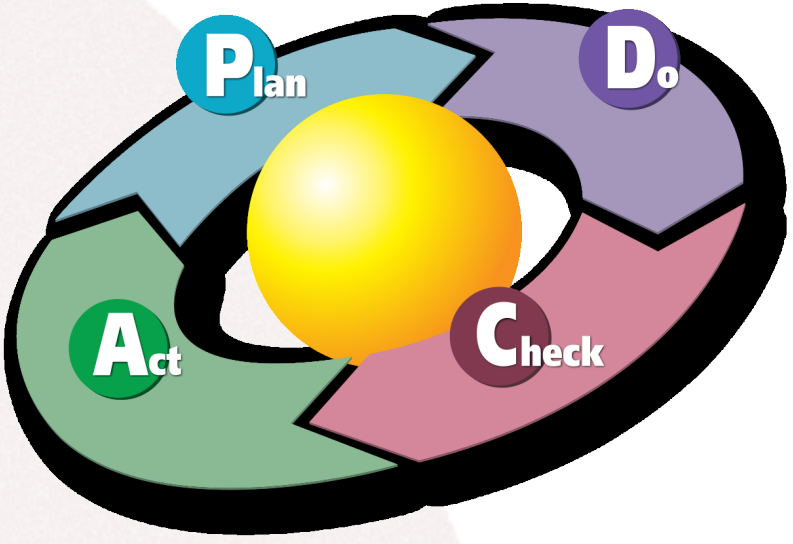


Avaliação do Risco

Título do Cenário						
Descrição						
FPC Afetado						
	Referência		Descrição			
Análise Inicial de Risco						
	Impacto	Serious	Probabilidade de Ocorrência	High	Known Security Risk	6
Controles						
	Mitigação de Impacto			Mitigação de Probabilidade		
Monitoração						
Recomendações Adicionais						
Análise de Risco Residual						
	Impacto	Serious	Probabilidade de Ocorrência	Medium	Planned Residual Security Risk	4

Análise de Vulnerabilidade

- Nessus e Nikto
- Avaliação de Risco
- Mitigação
- Chamados...



Hardening de Sistemas

- Objetivo Mór da *InfoSec* Quase Atingido
- Windows
  - Servidores
  - Estações
- Linux
- Bancos de Dados
  - Oracle
  - SQLServer

Hardening Windows

- P2V – Para Testes - Backup
- Métodos:
  - BIOS – GPO – Scripts (*sic!*) - WMI
  - Imagem de SO para Estações
- Serviços, Acessórios, NetBIOS, Permissões no System32, Adm, Políticas de Auditoria, Logs, Etc, Etc...

Hardening Linux
Bastille

```
# sudo apt-get install bastille
  # sudo bastille -x
  # bastille -c
  # sudo RevertBastille
```

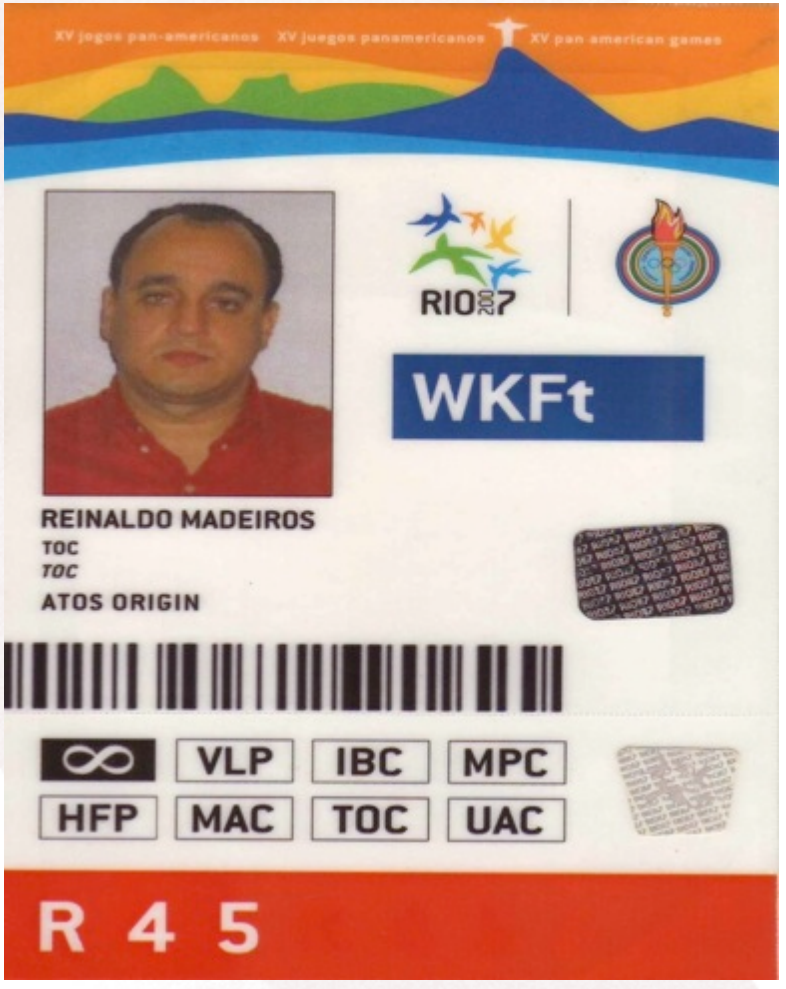
- No Site do Bastille:
  "January 29th, 2012: We are starting back up with active development! Stay tuned for news!"

Controle de Acessos

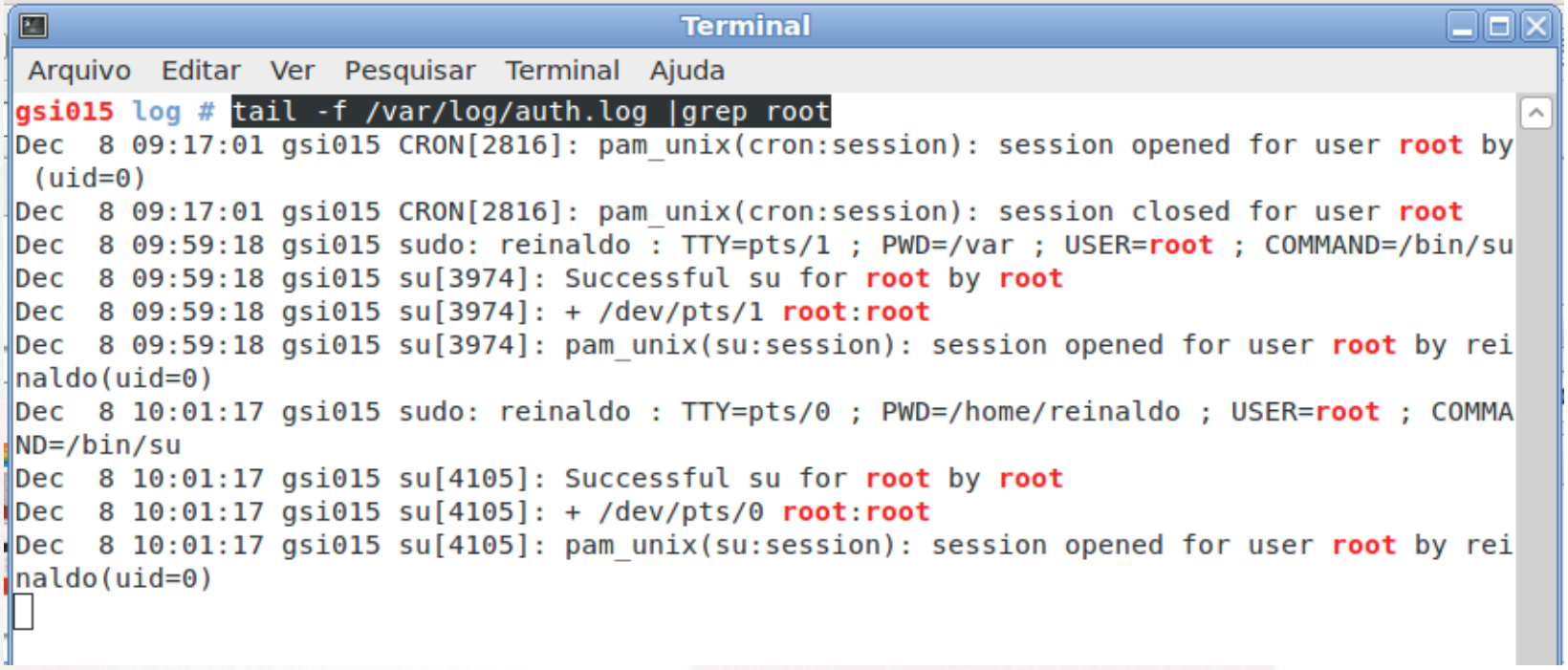
- Credencial
- RFID
- Sistemas dedicados de acreditação
- AD - Tacacs
- Relembrando:
  - 46 instalações
  - 15.000 voluntários
  - 3.000 jornalistas
  - 5.634 atletas de 42 países...

Controle de Acessos

Controle de Acessos



Análise de Logs - Quem Nunca?



SIEM - Sentinel

- Peça Chave Durante os Jogos
- Plano B - OSSIM
- Arquitetura baseada em *Syslog*
- Sensores Principais
  - *Switches*
  - IDS
  - *Syslogs*
- Correlação e Escalonamento de Eventos
- Integração ao *Service Desk*

Service Desk - TOP

- Desenvolvimento Interno
- ITIL
- Apoio à Segurança

TOC – Centro Nervoso dos Jogos

ABIN

- O Papel da ABIN
  - Moderação
  - Apoio em questões decisivas
  - Garantir que o que foi prometido seria entregue
  - Auditar e testar..

Ensaios Técnicos 1 e 2
Diversão

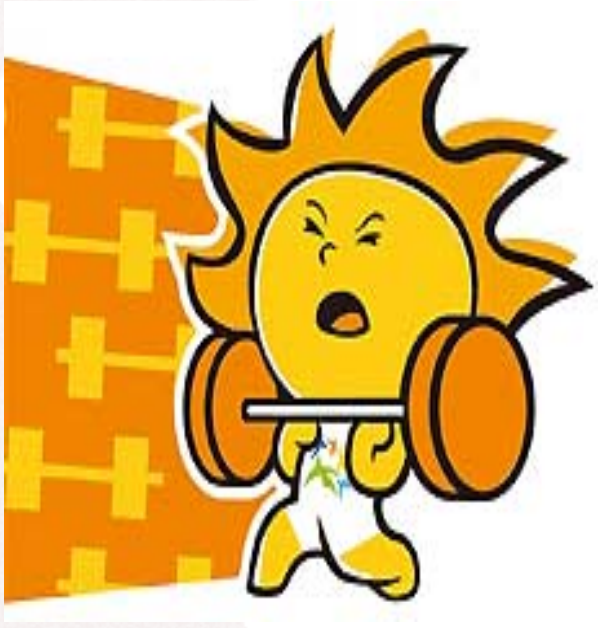
- *Failover* de *firewall* e do ISA
- Ping e *syn flood*
- Varredura de portas e busca por vulnerabilidades
- Roubo de IP, duplicação de MACs
- Conexão de dispositivos não autorizados
- SQL e URL *injection*
- Sabotagens internas...

A pressão durante os jogos

- Nada poderia falhar.
- Operadoras não podem integrar tecnologia de jogos:
- *"- Senhor Maratonista, o senhor <u>poderia estar correndo</u> novamente a maratona senhor? O sistema estava fora do ar senhor"*
- Vamos aos Incidentes...

Incidentes

- Antes do Jogos
  - *Moodle*
  - *Spam*
- Durante os Jogos
  - *Port security*
  - *Port scan* Conta?
- Quase nada aconteceu, ou não monitoramos direito



Resultado: Sucesso!!

- Tecnologia suportou o bom andamento dos Jogos
- Divulgação dos resultados com precisão
- Total disponibilidade dos aplicativos e portais
- Referência para Olimpíadas de Pequim
- NINGUÉM FALOU SOBRE TECNOLOGIA...

O Legado

- Tecnologia
- Metodologia
- Reflexão para os Jogos Olímpicos de 2016....
- Por um Legado de TI

Equipe – parcial!! - no Fim de Projeto

Obrigado

- Reinaldo de Medeiros
  - reinaldo@entalpia.com.br
  - reinaldo@reinaldo.org
  - Skype – ReiMed
  - Twitter: @ReiMedeiros
  - +55 21 8129-1545