

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 “Ensaio Técnico”
- 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

Men's 1,500m
Result - Semifinal 1

Rank	Country	Points	Name	Record	Time
1	BAR	375	John Smith	WR Q	3:21.32
2	CAN	274	Jean-Michael Bertrand	GR Q	3:21.46
3	BRA	464	Michael Saunders	Q	3:21.75
4	CUB	389	Walter Alexander	Q	3:22.47
5	JAM	202	Barry Johnson		3:24.32
6	BER	178	Bartholomew St John		3:25.60
7	PER	390	Alfredo Gonzalez		3:26.78
	VEN	631	Jose Antonio Ruiz	DSQ	

RIO 2007
Viva sua energia!

Rio 2007 em um clique buscar

4

re visitantes

Sabe o que faz sua vida mais gostosa?
Passe o mouse.

Calendário e Resultados

Calendário e Resultados

Esportes/Disciplina	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
Atletismo																		
Badminton																		
Basquetebol																		
Beisebol																		
Boliche																		
Boxe																		
Canoagem Velocidade																		
Ciclismo BMX																		

MEN'S DISCUS THROW
FINAL

Rank	Name	Country	WR	PR
1	ROBERTSON M.	USA	74.08	67.32
2	SLOWIK DARIUSZ	CAN	59.24	57.37
3	LASTRE YUNIO	CUB	54.80	54.80
4	JULIAO RONALD	BRA	53.54	53.54
5	KUEHL ADAM	USA	53.43	53.43
6	ANGULO JULIAN	COL	50.79	50.79
7	SHALLOW A.	VIN	50.61	50.61
8	LAURO GERMAN	ARG	50.58	50.58

TISSOT



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



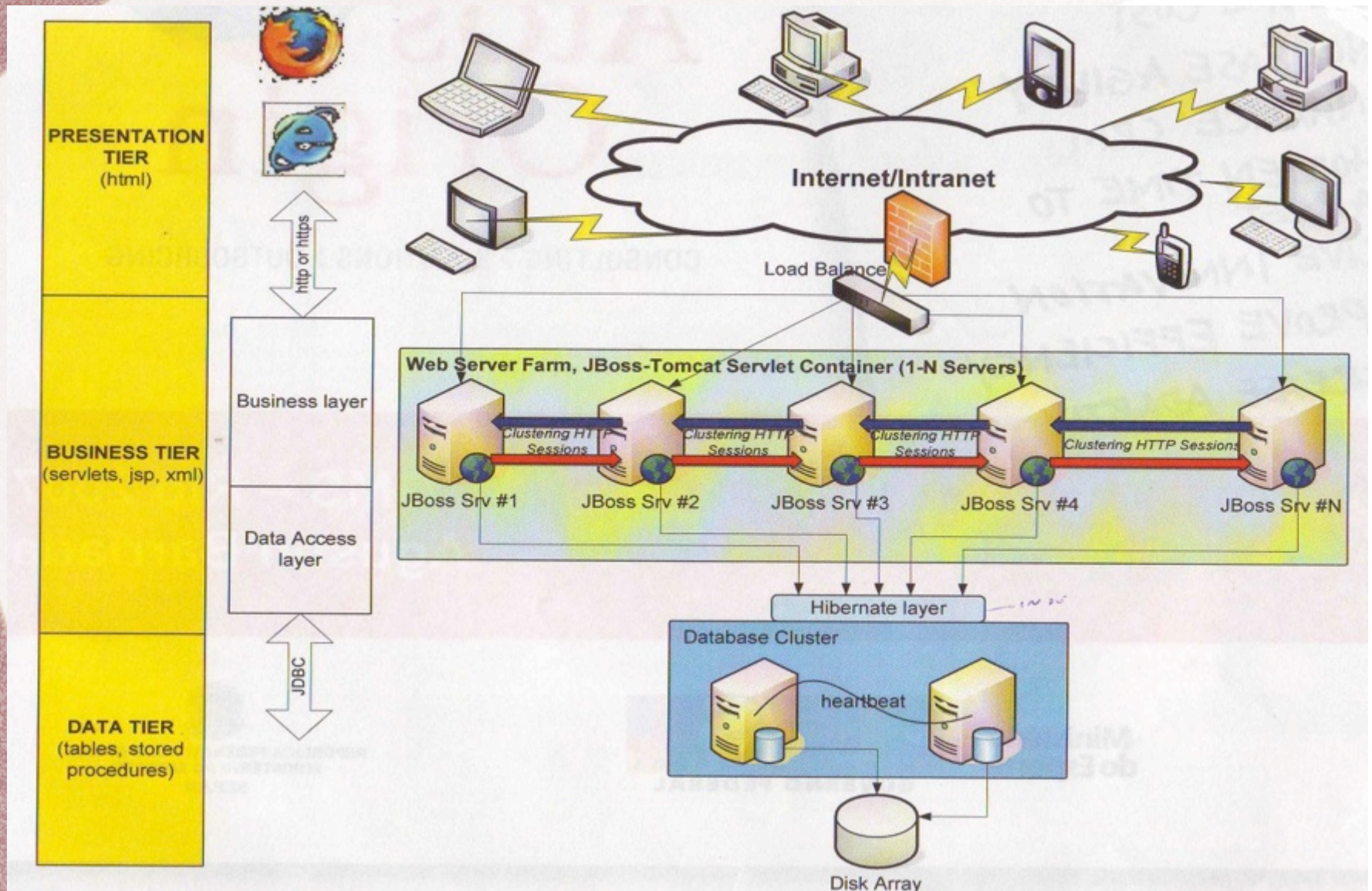
Sistemas Maduros



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



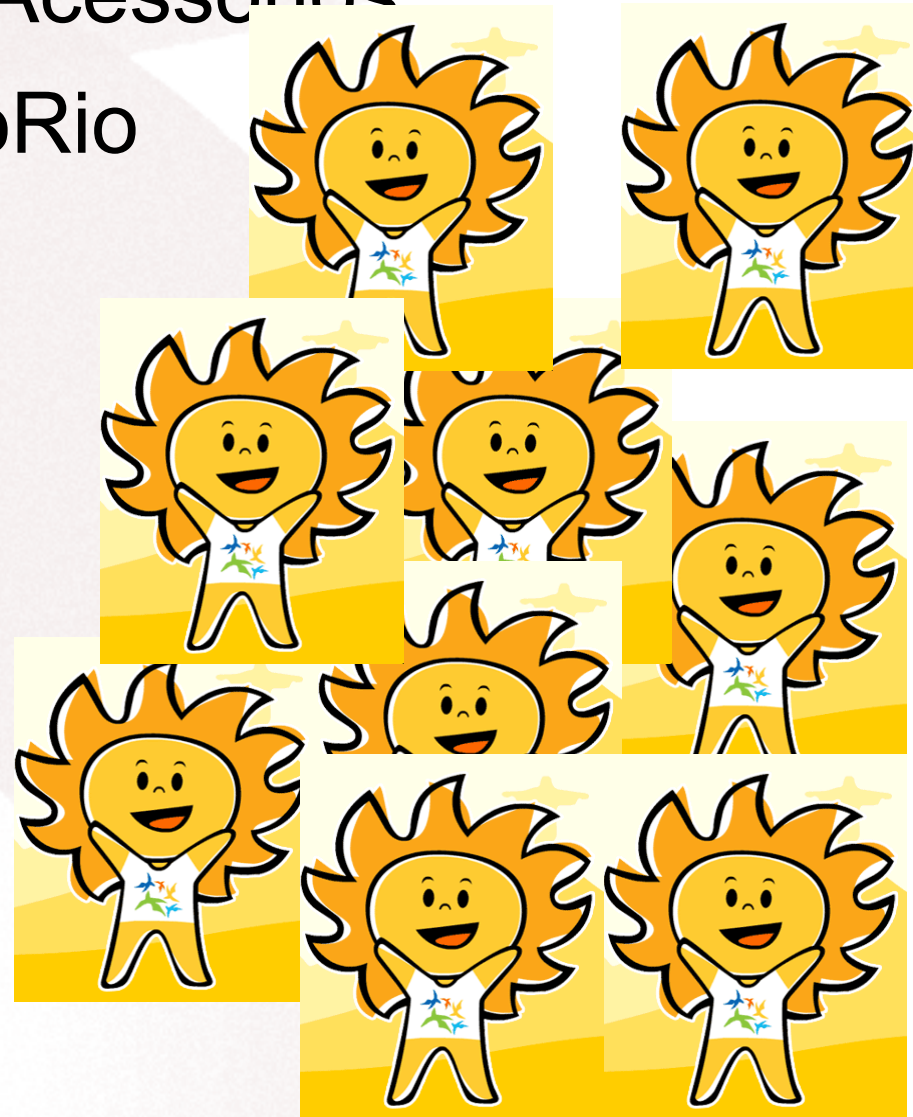
Pressão por prazos

- 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

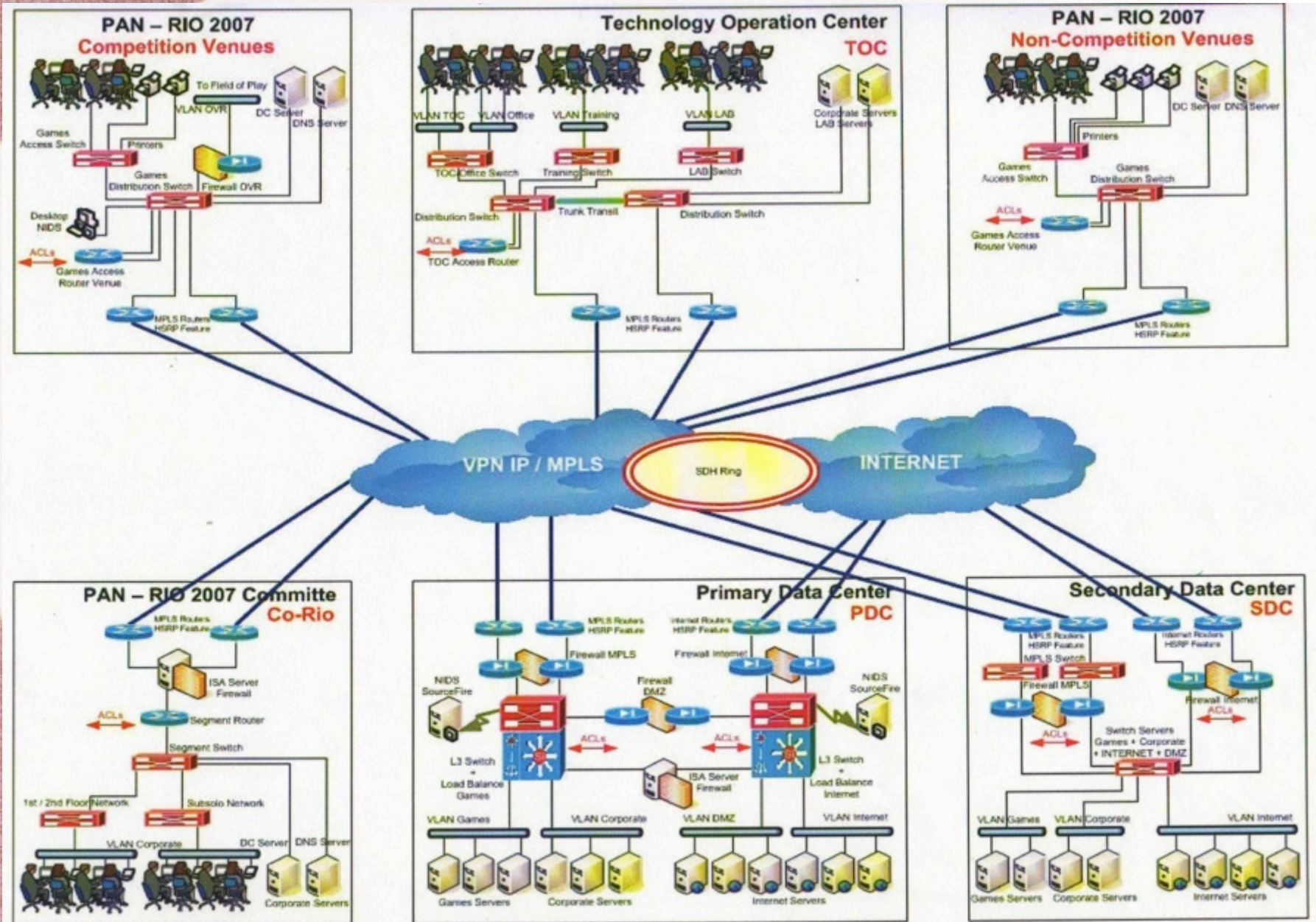
- Coordenador Arquitetura de Solução
Luciano Wulff
- Implementação e Operação
Kenia Gaipo -> Ivan Aquino
- Monitoramento e Incidentes
- Riscos e Vulnerabilidades
Reinaldo Medeiros

Infraestrutura ***“E Fez-se Luz”***

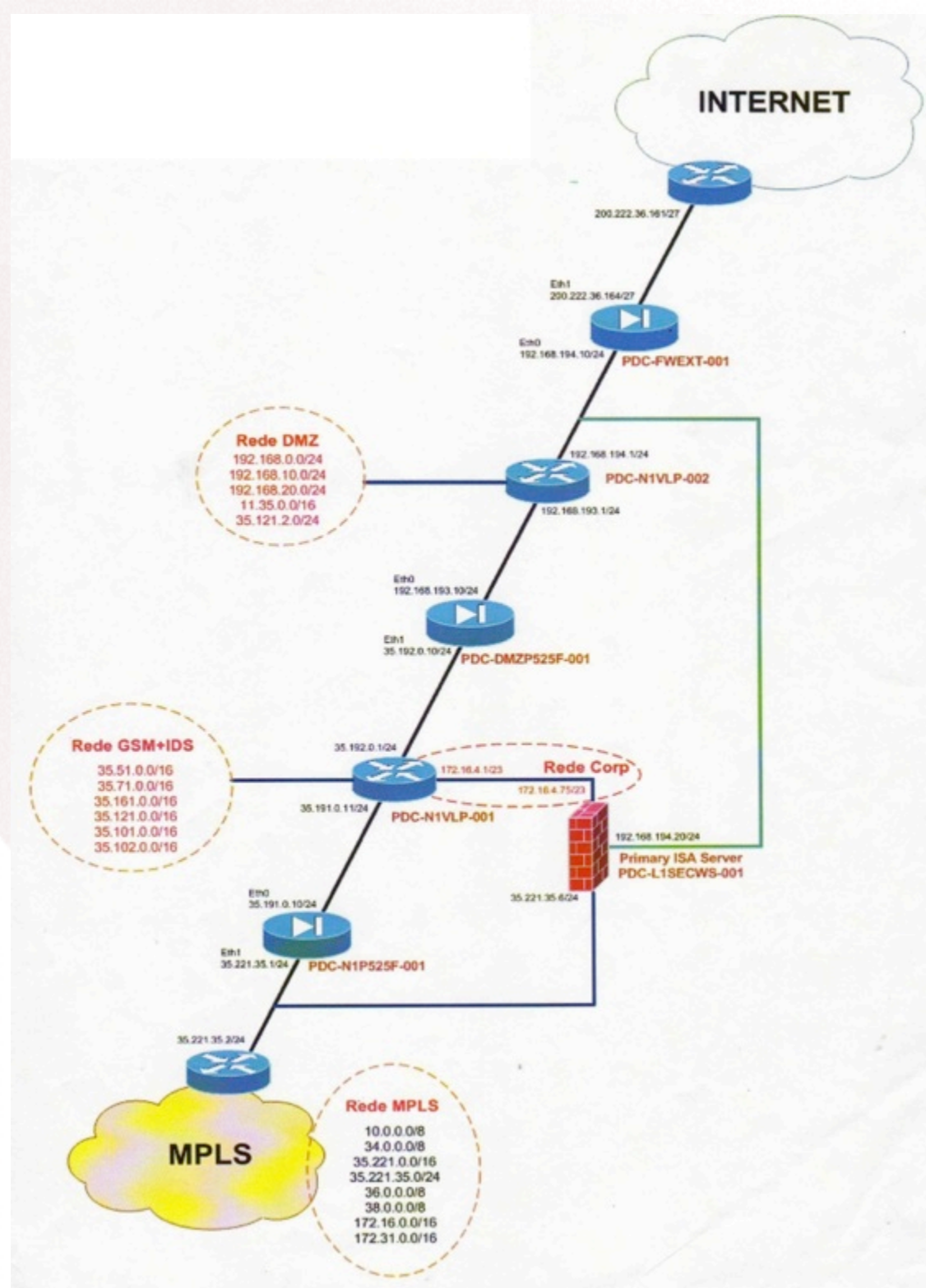
- Deus criou o mundo em 7 dias porque não havia usuário, base instalada e nem legado
- Desenhada do Zero
- *Hardware e software* padronizados
- Até infraestrutura *Windows* funciona bem...



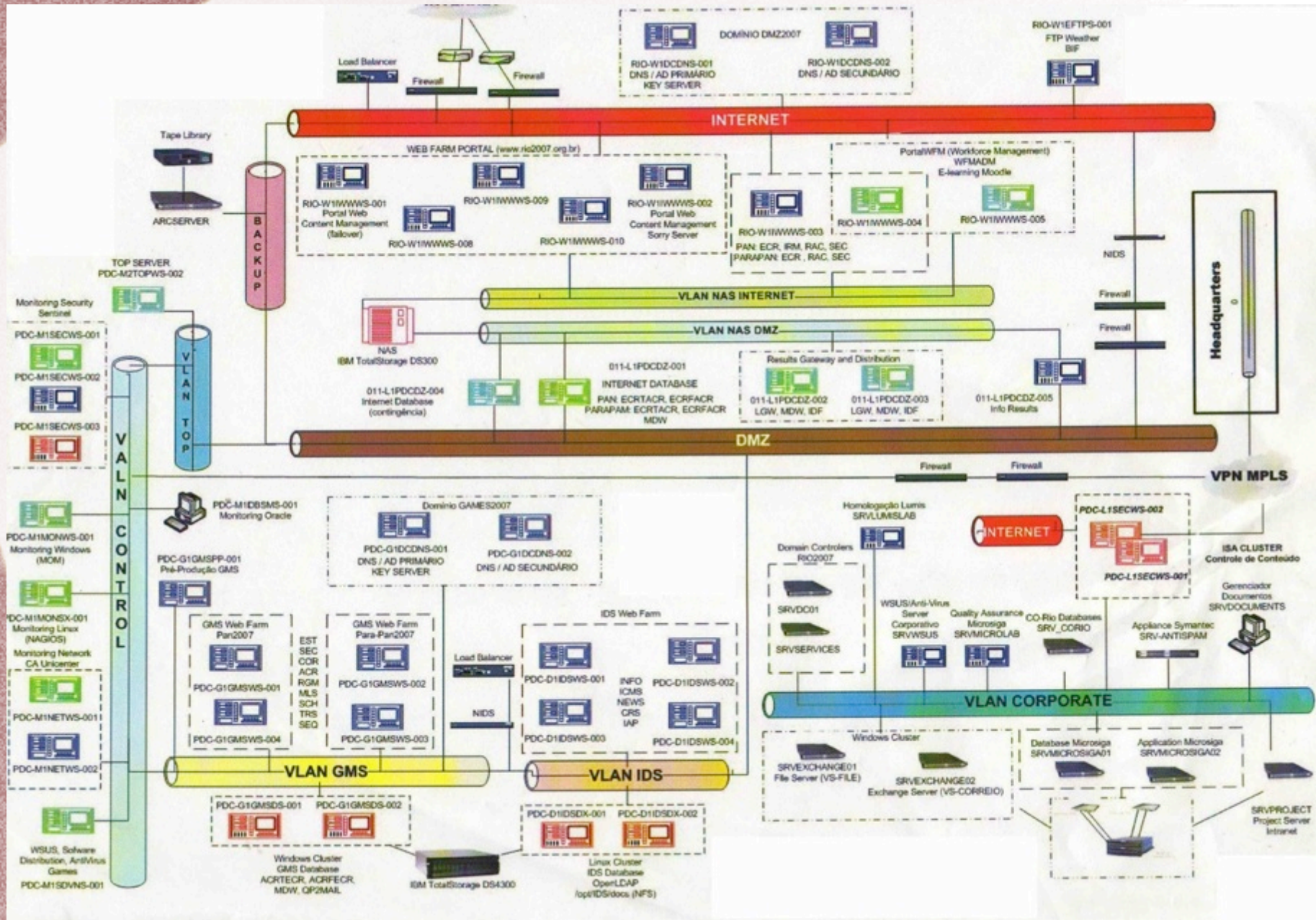
Arquitetura Física



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



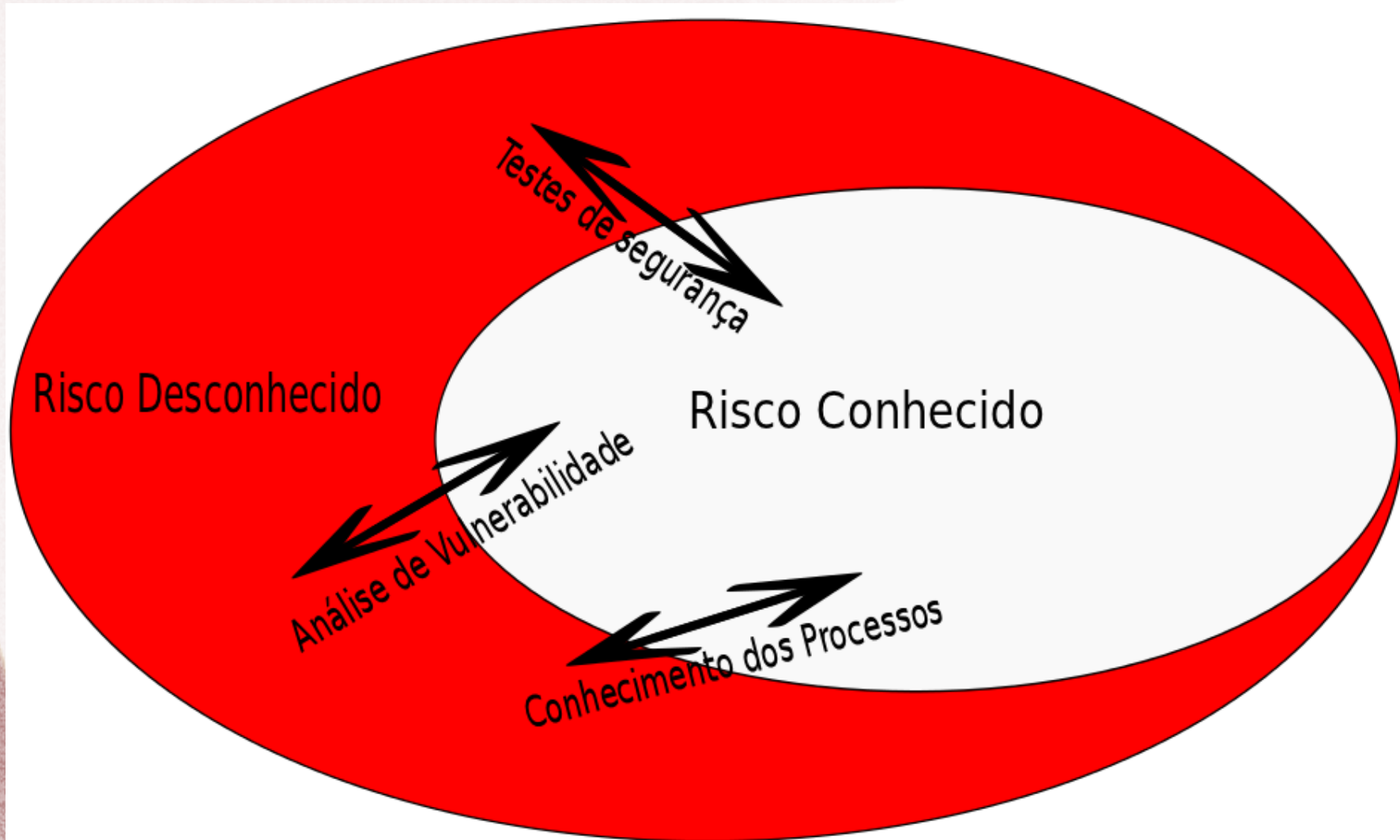
ALOG DATACENTERS - Unidade RJ

Citta America

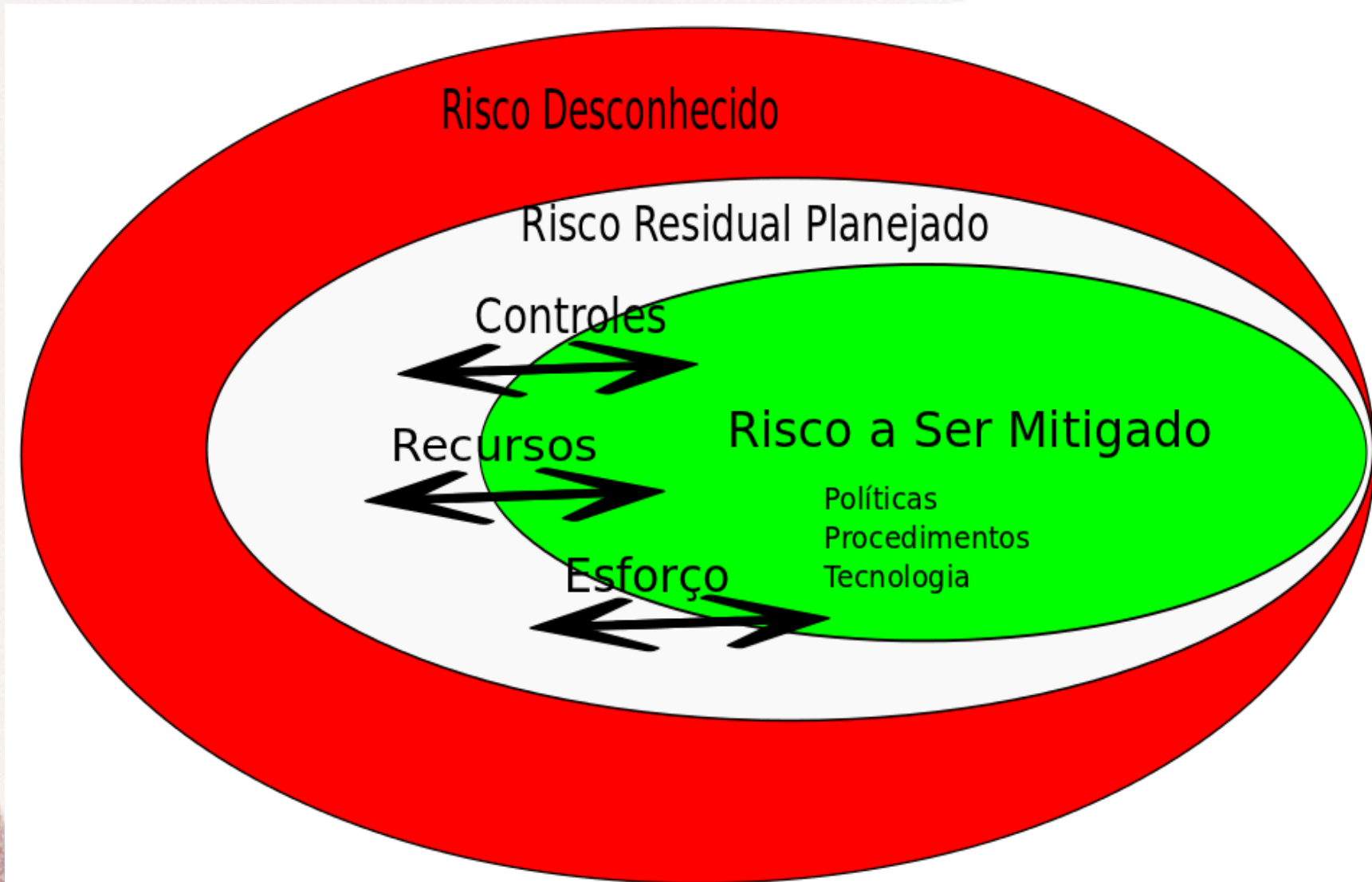
Gerenciamento de Risco

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

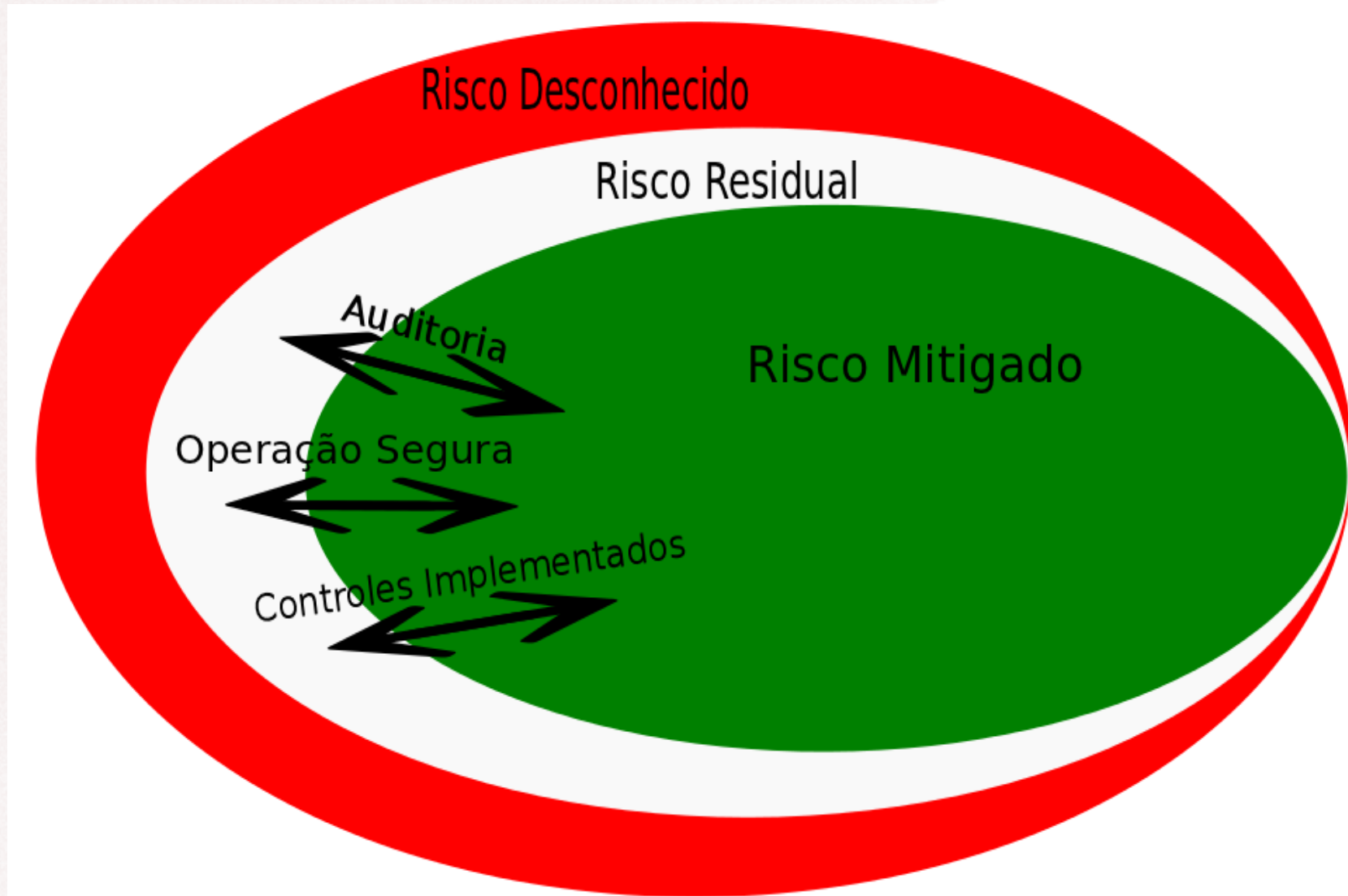
Risco Desconhecido vs Conhecido



Risco Mitigado



Gerenciamento de Risco

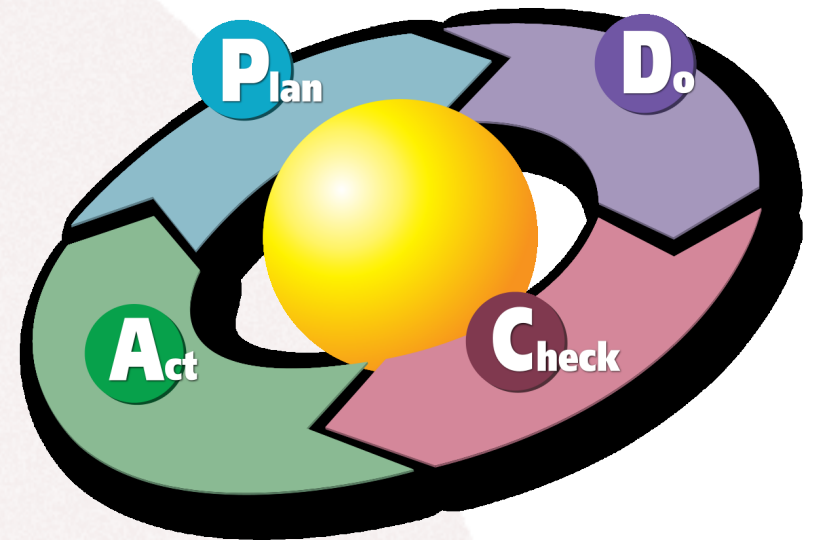


Avaliação do Risco

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

	TODAS AS INSTALAÇÕES ESPORTIVAS TODAS LAS INSTALACIONES DEPORTIVAS ALL COMPETITION VENUES
	ZONA INTERNACIONAL DA VILA ZONA INTERNACIONAL DE LA VILLA VILLAGE INTERNATIONAL ZONE
	CENTRO INTERNACIONAL DE RADIODIFUSÃO CENTRO INTERNACIONAL DE RADIODIFUSIÓN INTERNATIONAL BROADCAST CENTRE
	CENTRO PRINCIPAL DE IMPRENSA CENTRO PRINCIPAL DE PRENSA MAIN PRESS CENTER
	HOTEL OFICIAL DA FAMÍLIA ODEPA HOTEL OFICIAL DE LA FAMILIA ODEPA PAN AMERICAN FAMILY OFFICIAL HOTEL
	CENTRO PRINCIPAL DE CREDENCIAMENTO CENTRO PRINCIPAL DE ACREDITACIÓN MAIN ACCREDITATION CENTER
	CENTRO OPERACIONAL DE TECNOLOGIA CENTRO OPERACIONAL DE TECNOLOGÍA TECHNOLOGY OPERATIONS CENTER
	CENTRAL DE UNIFORME E CREDENCIAMENTO CENTRO DE UNIFORMES Y ACREDITACIÓN UNIFORM DISTRIBUTION AND ACCREDITATION CENTER
	ZONA RESIDENCIAL DA VILA ZONA RESIDENCIAL DE LA VILLA VILLAGE RESIDENTIAL ZONE

4

ÁREA RESERVADA PARA IMPRENSA
AREA DE PRENSA
PRESS AREAS

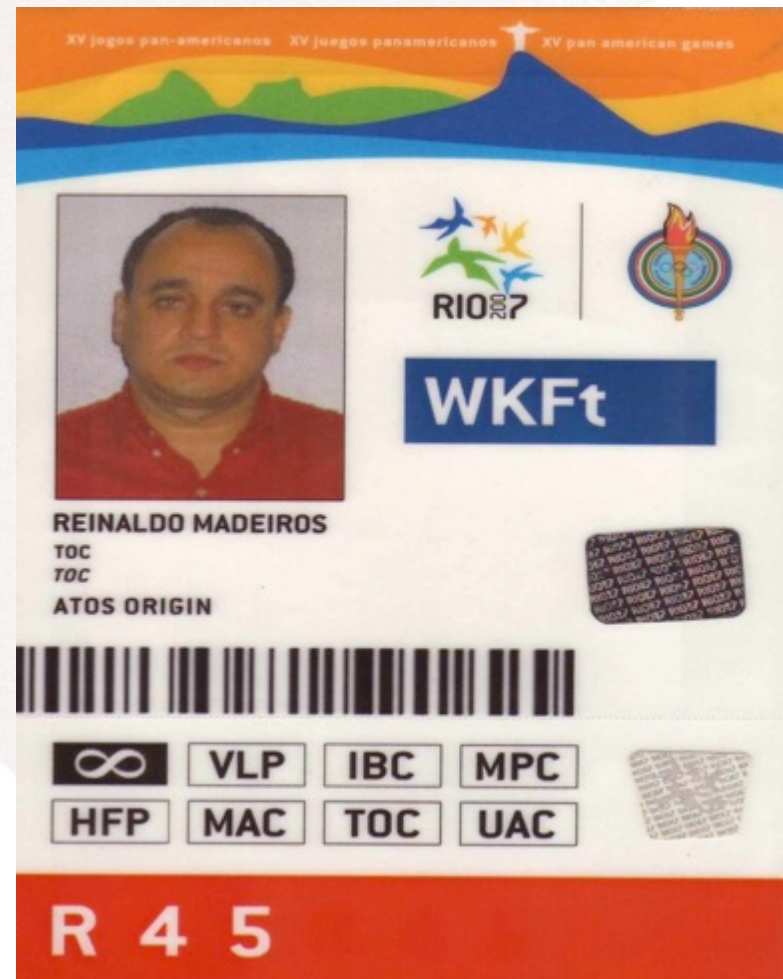
5

ÁREA RESERVADA PARA BROADCAST
AREA DE RADIODIFUSIÓN
BROADCAST AREAS

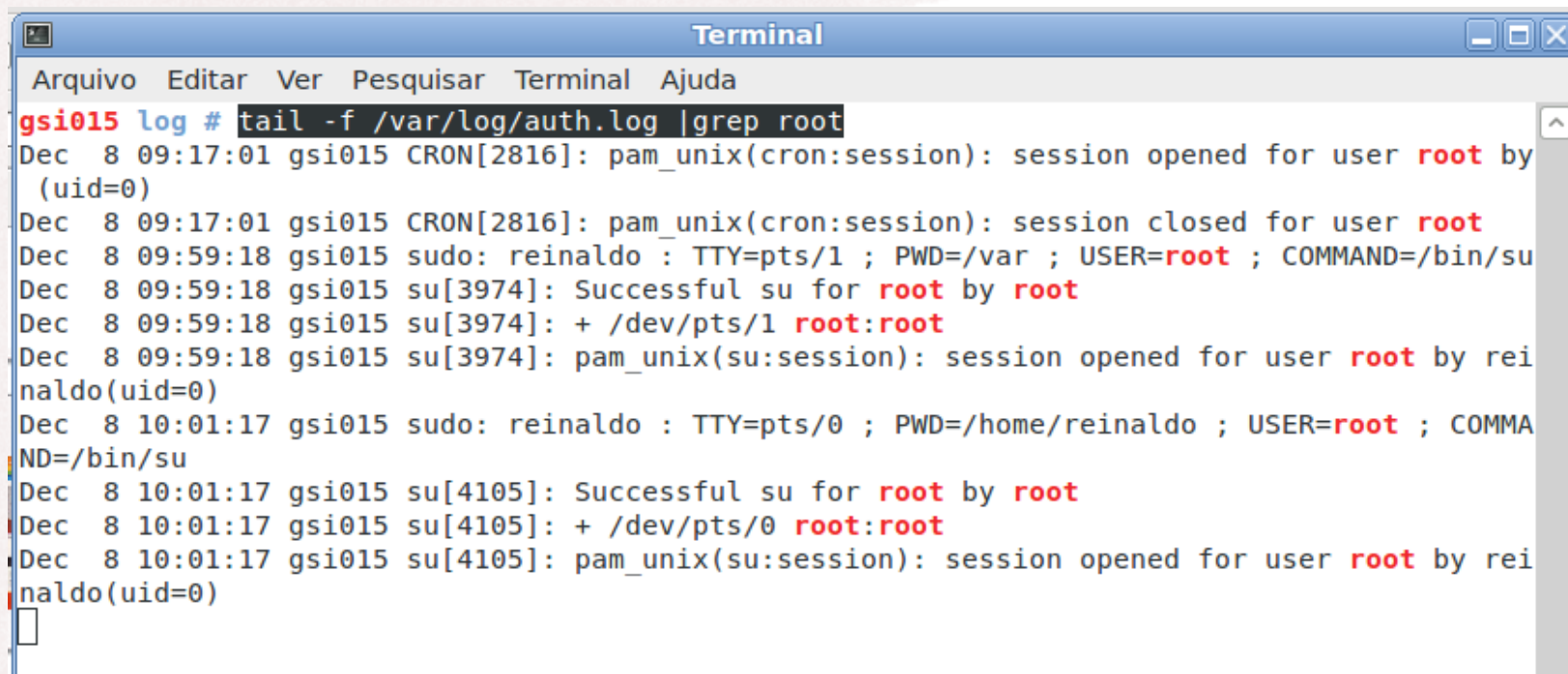


ÁREAS OPERACIONAIS
AREA OPERACIONAL
OPERATIONAL AREAS

Controle de Acessos



Análise de Logs - Quem Nunca?



```
Terminal
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
gsi015 log # tail -f /var/log/auth.log |grep root
Dec  8 09:17:01 gsi015 CRON[2816]: pam_unix(cron:session): session opened for user root by
(uid=0)
Dec  8 09:17:01 gsi015 CRON[2816]: pam_unix(cron:session): session closed for user root
Dec  8 09:59:18 gsi015 sudo: reinaldo : TTY=pts/1 ; PWD=/var ; USER=root ; COMMAND=/bin/su
Dec  8 09:59:18 gsi015 su[3974]: Successful su for root by root
Dec  8 09:59:18 gsi015 su[3974]: + /dev/pts/1 root:root
Dec  8 09:59:18 gsi015 su[3974]: pam_unix(su:session): session opened for user root by rei
naldo(uid=0)
Dec  8 10:01:17 gsi015 sudo: reinaldo : TTY=pts/0 ; PWD=/home/reinaldo ; USER=root ; COMMA
ND=/bin/su
Dec  8 10:01:17 gsi015 su[4105]: Successful su for root by root
Dec  8 10:01:17 gsi015 su[4105]: + /dev/pts/0 root:root
Dec  8 10:01:17 gsi015 su[4105]: pam_unix(su:session): session opened for user root by rei
naldo(uid=0)
```

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



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



Ensaaios 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...



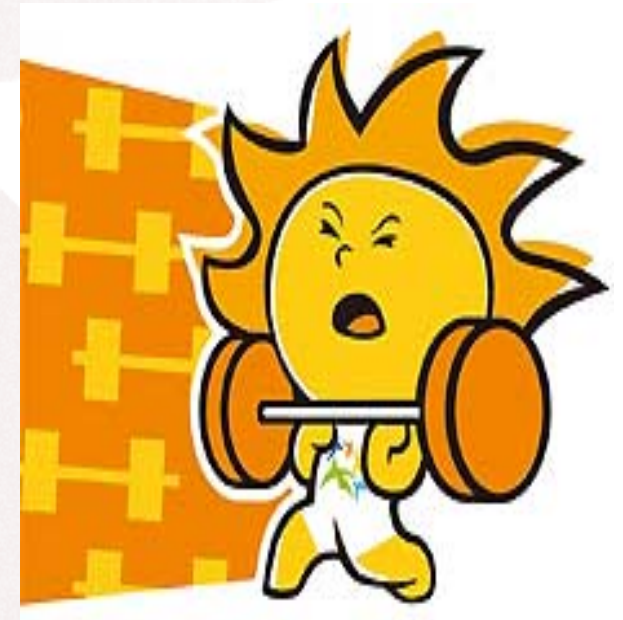
A pressão durante os jogos

- Nada poderia falhar.
- Operadoras não podem integrar tecnologia de jogos:
- “- *Senhor Maratonista, o senhor poderia estar correndo 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