Tecnologias de Segurança e Detecção de Vulnerabilidades em Sistemas de Automação Metroviária

Gilmario Ribeiro

Bruno Leça Ribeiro

20ª SEMANA DE TECNOLOGIA METROFERROVIÁRIA

AEAMESP

AEAMESP
Associação dos Engenheiros e Arquitetos de Metrô

20ª Semana de Tecnologia Metroferroviária 2014

PRÊMIO TECNOLOGIA & DESENVOLVIMENTO METROFERROVIÁRIOS 2014

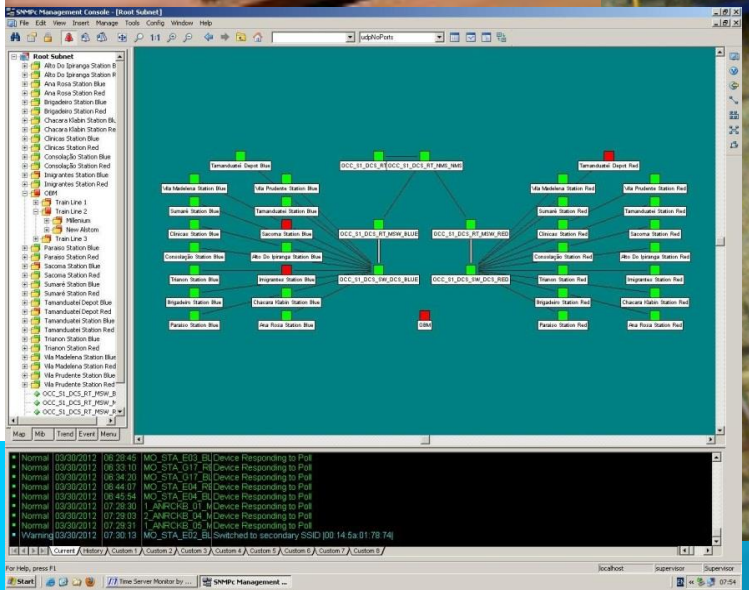
CBTU Companhia Brasileira de Trens Urbanos

ANPTrilhos

Tecnologia & Segurança

…uma Tecnologia nova quando surge, engole a outra…e ela tem que ser sempre a favor dos processos/pessoas...

Modernização tecnológica do ambiente metroviário



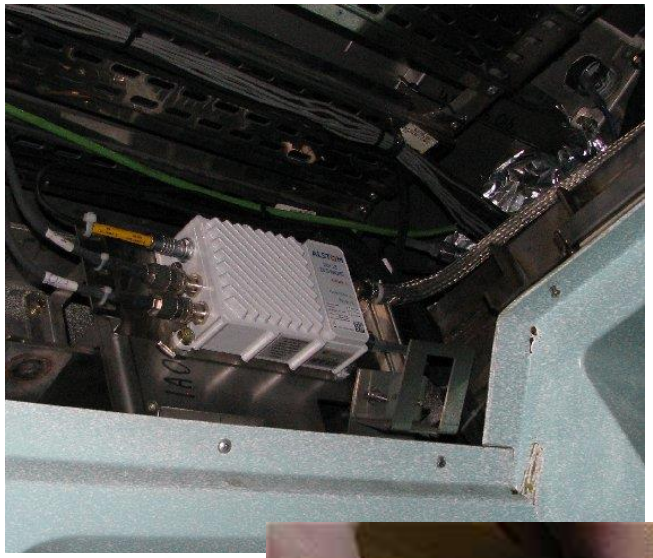
MANUTENÇÃO METROFERROVIÁRIA

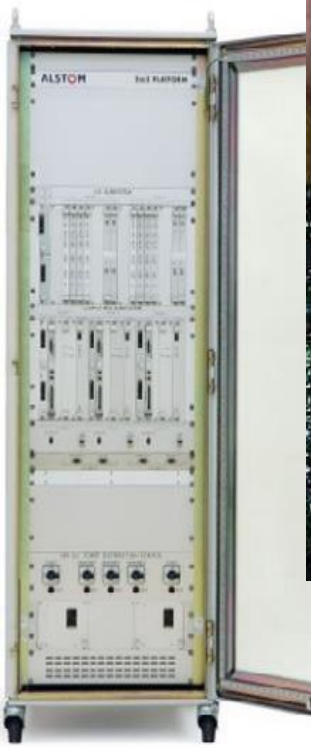
Assegurar a disponibilidade operacional dos equipamentos e instalações do Sistema Metroferroviário

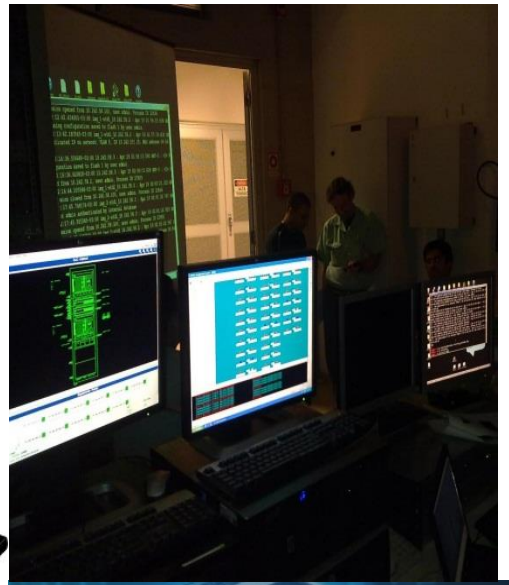
Tecnologia & Segurança

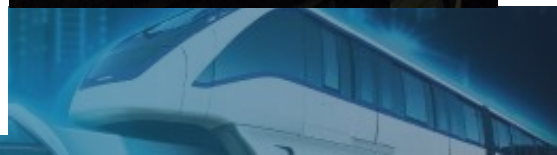
…quanto mais Tecnologia se implanta, mais necessidade há de investimentos em Segurança…devido as vulnerabilidades decorrentes desta mesma tecnologia…

Acervo Computacional = TI & TA

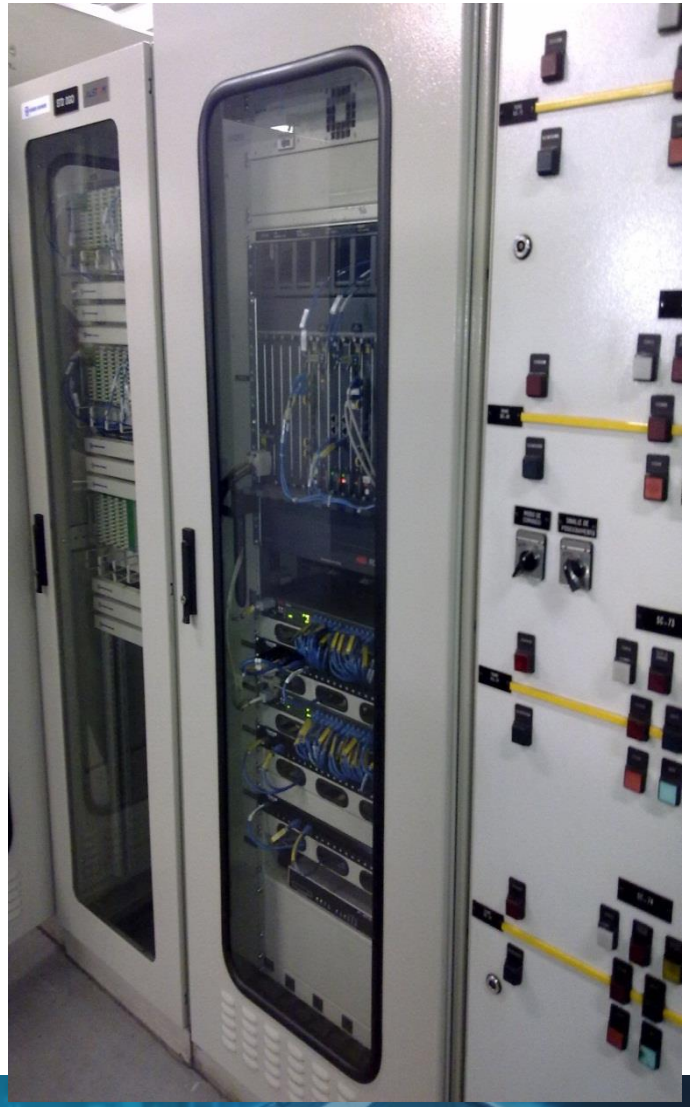








Acervo Computacional: necessita de gerenciamento constante



Interoperabilidade

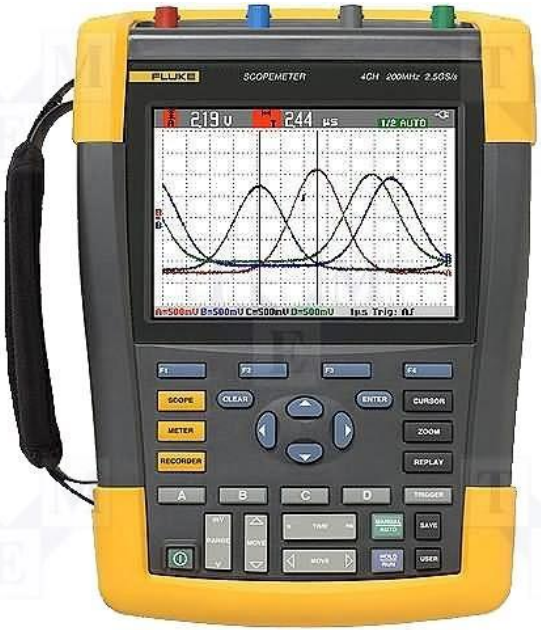
...incremento de novas tecnologias torna o gerenciamento das redes mais complexo, além disso, a interoperabilidade entre produtos de diferentes fabricantes é um obstáculo que deve ser superado...

Migração dos cenários

- Novos equipamentos, novas tecnologias
- Convergência do domínio analógico para cenários digitais
- Backbone = espinha do sistemas
- Equipamento em redes: cabo eletrônico, óptico ou Sem Fio
- Proporcional aumento de softwares e configurações
- Necessidade de integrações, gerência e monitoramento

Equipamentos ainda utilizados

As grandezas medidas eram tensão, corrente ou potência.



Osciloscópio Fluke 190-204

Multímetro Fluke 189

Convergência para o cenário de redes

Não existem grandezas físicas para serem medidas, somente lógicas

Link Runner Fluke

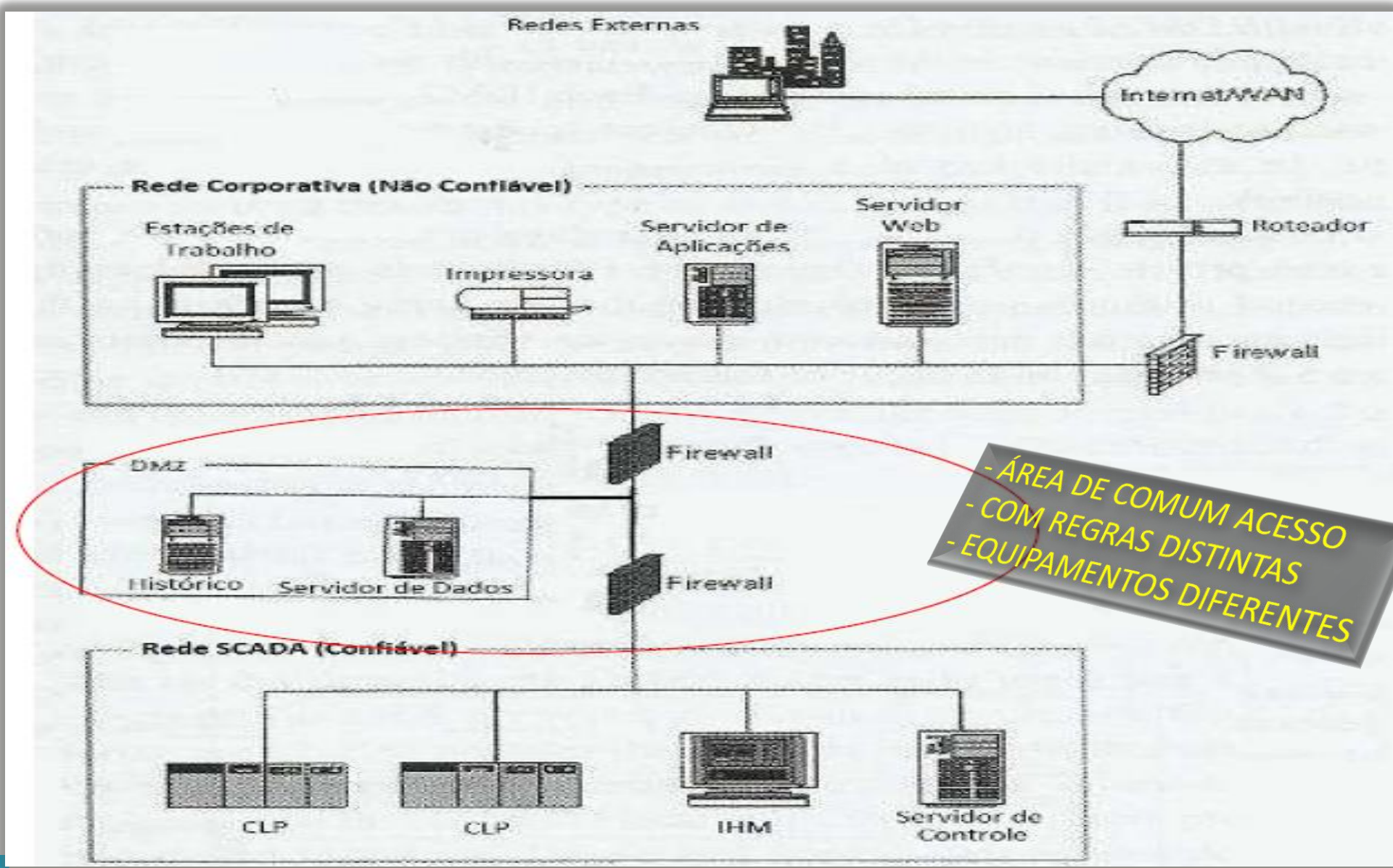
EtherScope - Fluke

Segurança em Automação

....para TA, alta disponibilidade é o mais relevante no pilar CID da Segurança da Informação.

....GIRS é solução para um monitoramento integrado de sistemas críticos em tempo real...

Ambientes Segregados (DMZ)



Crimes Cybernéticos

...os cyber crimes e as ameaças digitais correm na velocidade da LUZ e as ações envolvendo segurança andam na velocidade da LEI...

Sofisticação das Intrusões

FILME: *STUXNET (3,20 min)*

...virus em ambiente de automação...

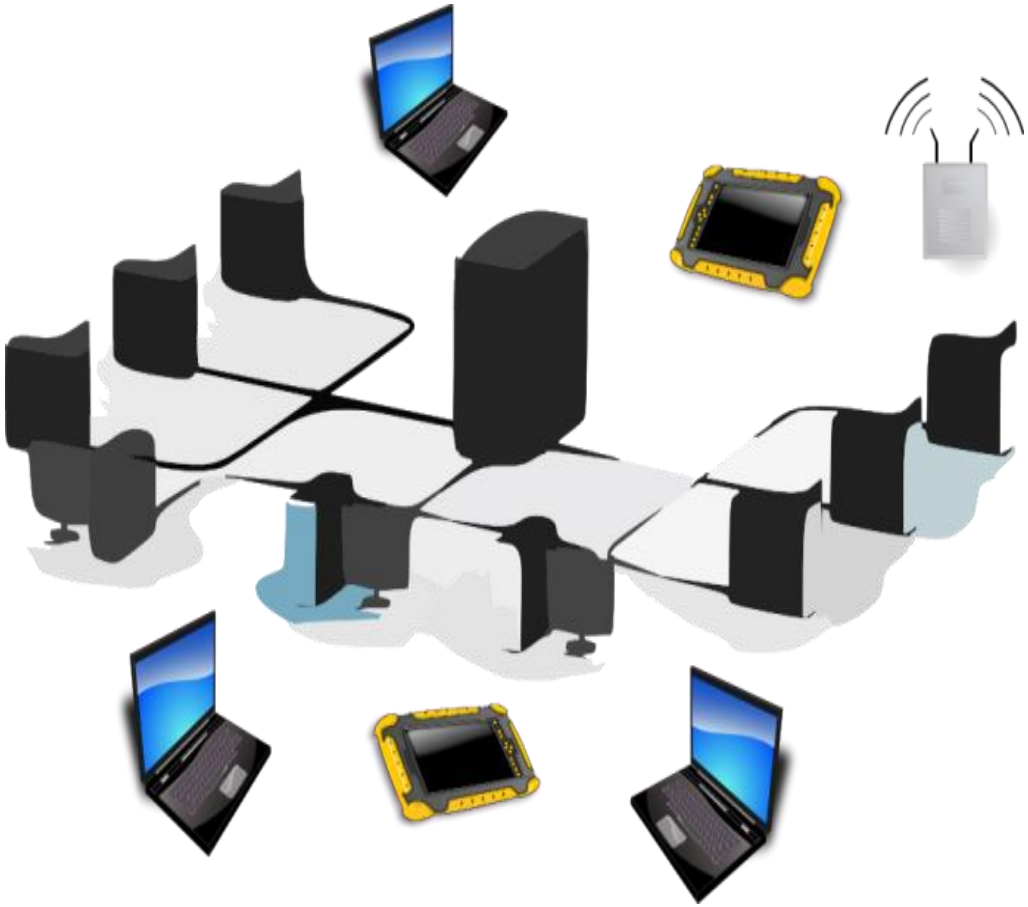
Inércia & Acomodação

...só aplicam-se regras rígidas de Segurança, apenas em 2 momentos:

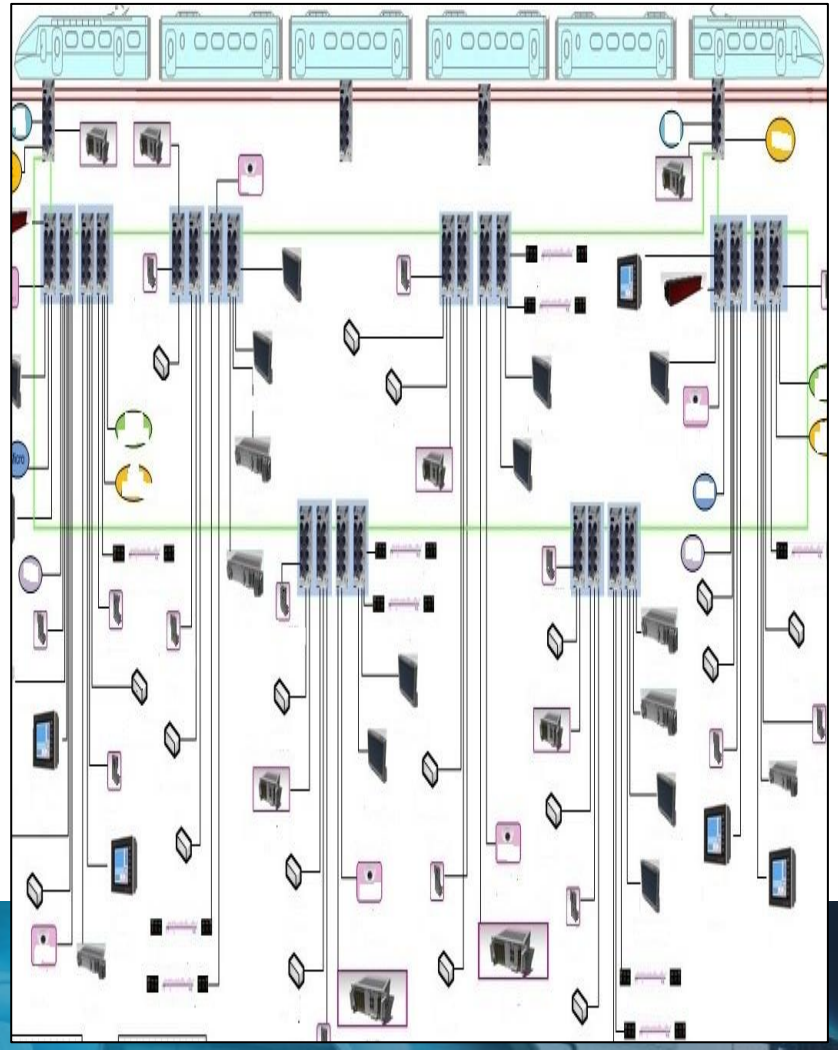
1 *- Quando em experiências traumáticas ou;*

2 *- Sob força da Lei.*

Redes Locais e Embarcadas



(Wan, Lan, Wlan, Scada)



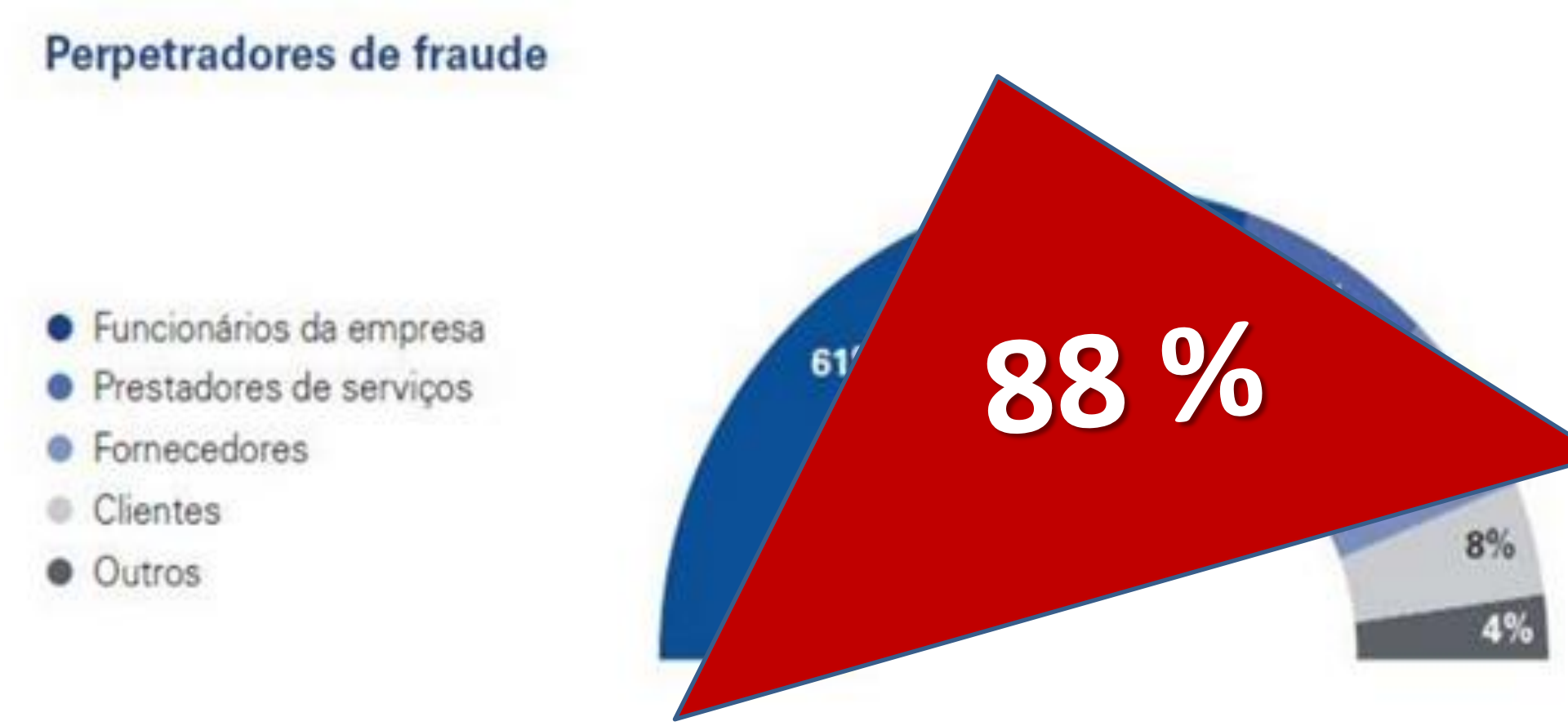
Missão Crítica (Safety)

...em missão crítica, a ausência das políticas de governança e de segurança, faz com que as pessoas adotem suas próprias medidas, podendo ter então, resultados catastróficos...

Alvos Atrativos

Vulnerabilidades

Riscos, Ameaças, Ataques, Invasões, Impactos, Danos



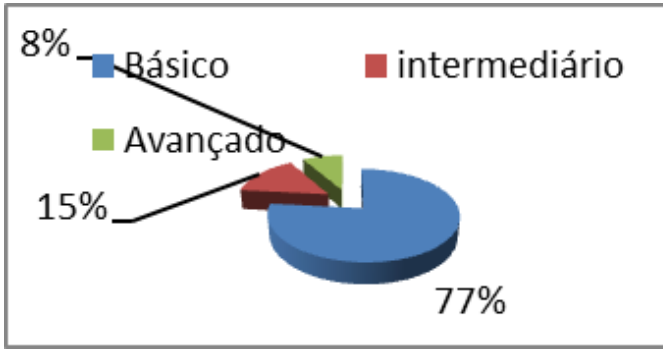
- **SEGURANÇA** = **SAFETY & SECURITY**

Fonte: KPMG – A Fraude no Brasil – Relatório da Pesquisa 2009
http://www.kpmg.com.br/publicacoes/forensic/Fraudes_2009_port.pdf

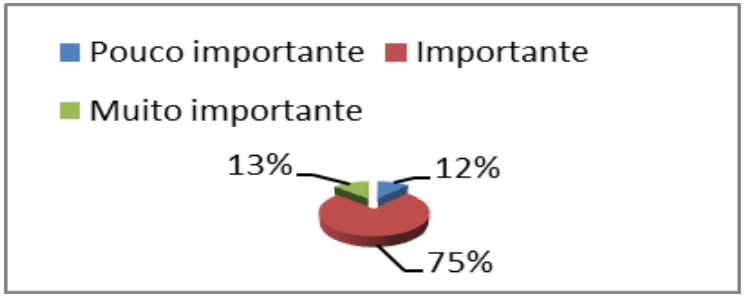
Pesquisa Técnica em Ambiente de Automação

Fonte: Centro Universitário FEI - SP

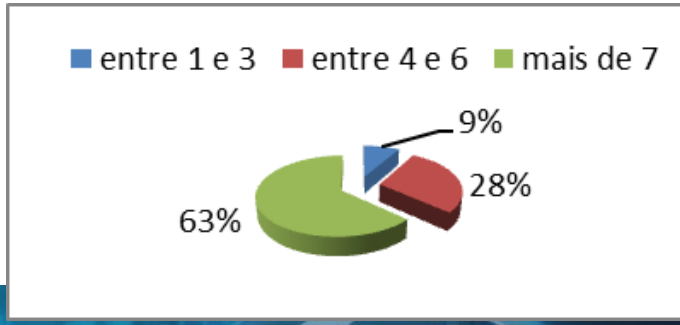
1) Qual seu conhecimento em redes de computadores?



2) Qual a importância do conhecimento de redes no seu dia-a-dia?



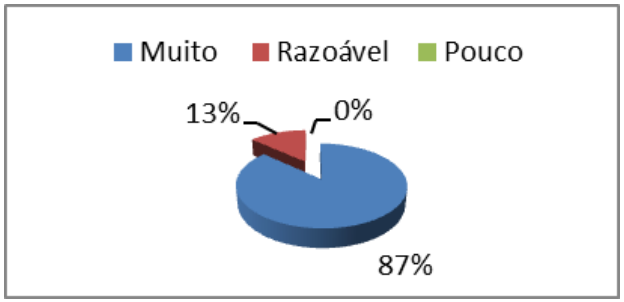
3) Qual da média de equipamentos que você atua que têm redes?



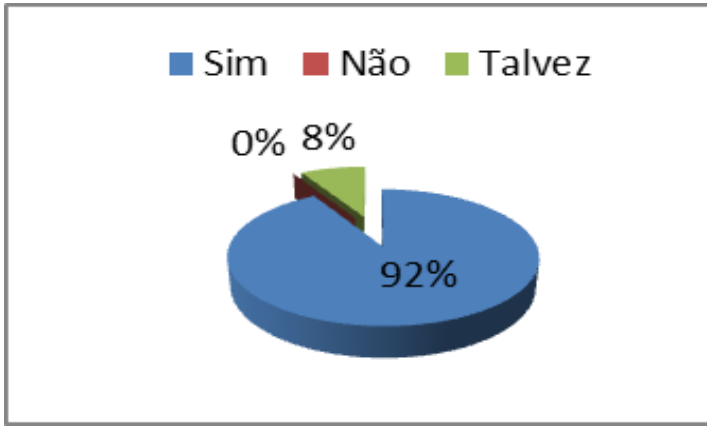
Pesquisa Técnica em Ambiente de Automação

Fonte: Centro Universitário FEI - SP

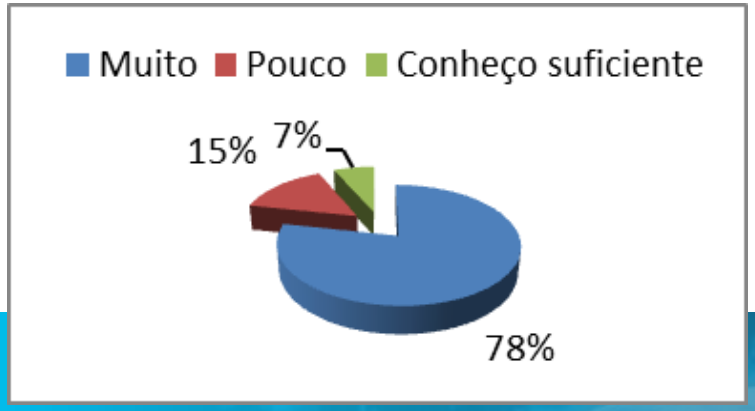
4) Quanto os conhecimentos em redes ajudaria no atendimento de falhas destes equipamentos?



5) Você acha que a tecnologia está migrando para os equipamentos de rede?



6) Para você o quanto falta no conhecimento em redes?



Recomendações: Cenário ideal

- **Centro Integrado de Operações das Redes e Sistemas (Gerenciamento e Monitoramento via NOC/SOC com IDPS)**
- Criação de um CSIRT - Centro de Respostas a Incidentes de Segurança
  - Tratamento de todas as Vulnerabilidades mapeadas
  - Promoção da cultura em Segurança Física e Lógica (envolvendo Safety & Security)
- Capacitação permanente do Corpo Técnico envolvido
- Governança em Segurança da Informação e de Automação

COMMIT

Modelo de Gerência

Centro de Operaciones de Mantenimiento y Monitorización de Instalaciones y Telecomunicaciones

Metro de Madrid, S.A.
Consultoría de Proyectos

Recomendações: Cenário ideal

- *Centro Integrado de Operações das Redes e Sistemas* √
  (Gerenciamento e Monitoramento - NOC / SOC)

- **Criação de um CSIRT - Centro de Respostas a Incidentes de Segurança**
  - Tratamento de todas as Vulnerabilidades mapeadas
  - Promoção da cultura em Segurança Física e Lógica (envolvendo Safety & Security)

- Capacitação permanente do Corpo Técnico envolvido

- Governança em Segurança da Informação e de Automação

CSIRT- Centro de Respostas e Incidentes de Segurança

- Grupo multidisciplinar...
- Implantação de Políticas...
- Analisar / tratar ocorrências de segurança...
- Promover cultura interna de segurança...

...a pior Segurança,

é aquela em que se ACHA, que JÁ estamos totalmente seguros...

Recomendações: Cenário ideal

- *Centro Integrado de Operações das Redes e Sistemas (Gerenciamento e Monitoramento - NOC / SOC)* √
- *Criação de um CSIRT - Centro de Respostas a Incidentes de Segurança* √
  - *Tratamento de todas as Vulnerabilidades mapeadas* √
  - *Promoção da cultura em Segurança Física e Lógica (envolvendo Safety & Security)* √
- **Capacitação permanente do Corpo Técnico envolvido**
- Governança em Segurança da Informação e de Automação

Treinamentos de capacitação constante

- **Conhecimento Básico de Redes**

- **Conhecimento Avançado de Redes**

- **Gerenciamento e Segurança de TI & TA (TMN)**
  Telecommunications Management Network

Recomendações: Cenário ideal

- *Centro Integrado de Operações das Redes e Sistemas (Gerenciamento e Monitoramento - NOC / SOC)* √
- *Criação de um CSIRT - Centro de Respostas a Incidentes de Segurança* √
  - *Tratamento de todas as Vulnerabilidades mapeadas* √
  - *Promoção da cultura em Segurança Física e Lógica (envolvendo Safety & Security)* √
- *Capacitação permanente do Corpo Técnico envolvido* √
- **Governança em Segurança da Informação e de Automação**

Governança do acervo tecnológico
(dados e infraestrutura)

- **Integração segura dos ambientes de TI (administrativo) e de TA (automação)**

- **Sistema de Gestão de Segurança da Informação (SGSI)**

- **Certificações em segurança (ISO 27000 , ISA-99 etc)**

...NÃO existe a Segurança 100 % ...

http://www.sicherheitstacho.eu/?lang=en

http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&time=16235&view=map

http://www.tecmundo.com.br/seguranca/46926-estacao-espacial-internacional-e-infectada-com-o-virus-stuxnet.htm

Sofisticação das Intrusões

F I L M E: *Sabotagem digital* *(3,57 min)*

...ataques em sistemas críticos...

Tecnologias de Segurança e Detecção de Vulnerabilidades em Sistemas de Automação Metroviária

Gilmario Ribeiro

Bruno Leça Ribeiro

Obrigado

20ª Semana de Tecnologia Metroferroviária 2014

AEAMESP
Associação dos Engenheiros e Arquitetos de Metrô

gilribeiro@metrosp.com.br

bruno.lribeiro@metrosp.com.br